SECURING U.S. SURFACE TRANSPORTATION FROM CYBER ATTACKS

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY

AND THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

FEBRUARY 26, 2019

Serial No. 116–2

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov/

U.S. GOVERNMENT PUBLISHING OFFICE
35–378 PDF WASHINGTON : 2019

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
CEDRIC L. RICHMOND, Louisiana
DONALD M. PAYNE, JR., New Jersey
KATHLEEN M. RICE, New York
J. LUIS CORREA, California
XOCHITL TORRES SMALL, New Mexico
MAX ROSE, New York
LAUREN UNDERWOOD, Illinois
ELISSA SLOTKIN, Michigan
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
YVETTE D. CLARKE, New York
DINA TITUS, Nevada
BONNIE WATSON COLEMAN, New Jersey
NANETTE DIAZ BARRAGÁN, California
VAL BUTLER DEMINGS, Florida

MIKE ROGERS, Alabama
PETER T. KING, New York
MICHAEL T. MCCAUL, Texas
JOHN KATKO, New York
JOHN RATCLIFFE, Texas
MARK WALKER, North Carolina
CLAY HIGGINS, Louisiana
DEBBIE LESKO, Arizona
MARK GREEN, Tennessee
VAN TAYLOR, Texas
JOHN JOYCE, Pennsylvania
DAN CRENSHAW, Texas
MICHAEL GUEST, Mississippi

HOPE GOINS, *Staff Director*
CHRIS VIESON, *Minority Staff Director*

SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY

J. LUIS CORREA, California, *Chairman*

EMANUEL CLEAVER, Missouri
DINA TITUS, Nevada
BONNIE WATSON COLEMAN, New Jersey
NANETTE DIAZ BARRAGÁN, California
VAL BUTLER DEMING, Florida
BENNIE G. THOMPSON, Mississippi *(ex officio)*

DEBBIE LESKO, Arizona, *Ranking Member*
JOHN KATKO, New York
JOHN RATCLIFFE, Texas
MARK GREEN, Tennessee
MIKE ROGERS, Alabama *(ex officio)*

ALEX MARSTON, *Subcommittee Staff Director*
KYLE KLEIN, *Minority Subcommittee Staff Director*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

CEDRIC L. RICHMOND, Louisiana, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
KATHLEEN M. RICE, New York
LAUREN UNDERWOOD, Illinois
ELISSA SLOTKIN, Michigan
BENNIE G. THOMPSON, Mississippi *(ex officio)*

JOHN KATKO, New York, *Ranking Member*
JOHN RATCLIFFE, Texas
MARK WALKER, North Carolina
VAN TAYLOR, Texas
MIKE ROGERS, Alabama *(ex officio)*

MOIRA BERGIN, *Subcommittee Staff Director*
SARAH MOXLEY, *Minority Subcommittee Staff Director*

CONTENTS

SECURING U.S. SURFACE TRANSPORTATION FROM CYBER ATTACKS

Tuesday, February 26, 2019

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY, AND THE
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION AND INNOVATION,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The subcommittees met, pursuant to notice, at 10:03 a.m., in room 310, Cannon House Office Building, Hon. J. Luis Correa [Chairman of the Subcommittee on Transportation and Maritime Security] presiding.

Present: Representatives Correa, Richmond, Cleaver, Jackson Lee, Langevin, Watson Coleman, Rice, Barragán, Underwood, Slotkin, Lesko, Walker, and Taylor.

Also present: Representative Thompson.

[Editor's Note.—Due to technical difficulties, audible portions of this transcript were not recorded and those instances have been marked accordingly.]

Mr. CORREA. Good morning everyone. Seeing the time of 10:05 having arrived, I would like to gavel down and chair—and call the Subcommittees on Transportation and Maritime Security, and Cybersecurity, Infrastructure Protection, and Innovation, to order.

Today's hearing marks the first hearing of this Congress for the Subcommittee on Transportation and Maritime Security. I am excited to be chairing this subcommittee in this Congress and to be joined by our Ranking Member, Congresswoman Lesko from Arizona; I understand she is getting snow in Arizona, that is——

Mrs. LESKO. Right, that is—we were. It was crazy——

Mr. CORREA. You were?

Mrs. LESKO. In Phoenix.

Mr. CORREA. Save the water.

We have a great panel of distinguished Members on both sides of the aisle and I look forward to working with all of you to tackle the security challenges facing the transportation and maritime sectors.

I am glad to hold our first hearing, jointly with the Cybersecurity Subcommittee, and its leaders, Chairman Richmond, and Ranking Member Katko, who, Mr. Katko, unfortunately is not able to join us today.

I am also happy to welcome our two panels today of witnesses and I look forward to your testimony.

We are here today to discuss a very important topic: Cybersecurity in our Nation's mass transit, rail, pipeline, and other surface transportation systems. Cyber threats are a growing concern for security experts across many sectors and the surface transportation sector is no different. Millions of Americans, we rely on surface transportation every day and an attack against a large subway system or pipeline could have hugely negative effects on all of us.

Government and industry have both struggled to address cyber threats which have evolved quickly and have become more and more complex and I believe DHS is well-positioned to lead cybersecurity in the efforts across critical infrastructure sectors including the surface transportation sector.

Last year, Congress established a Cybersecurity Infrastructure and Security Agency, or CISA, making clear its status as the preeminent Cybersecurity Agency within the Federal Government. CISA works closely with TSA which is responsible for securing all modes of transportation. In December 2018 working with CISA, TSA released a Cybersecurity Roadmap that sets priorities for securing transportation from cyber threats.

The Roadmap is an important first step in the right direction, but it has to be followed by concrete action. In coordination with CISA, TSA must ensure owners and operators have access to the resources, intelligence, guidelines, and assessments needed to ensure the cybersecurity of their systems is as good as it can get.

Government and industry stakeholders together must also address supply chain security concerns. We must make sure that surface transportation systems are not made vulnerable to cyber espionage due to unchecked foreign manufacturing of subways [inaudible] some have questioned whether DHS has paid enough attention to Pipeline security and have raised the idea of moving the responsibility from securing pipelines to another department and Ms. Proctor I do hope you address that issue during your comments [inaudible] because it would go against the reasons Congress established DHS, TSA, and CISA.

Only DHS has the scope of authorities and access to intelligence needed to address cyber threats across critical infrastructure sectors. DHS has made significant progress in securing pipelines, including recent updates of TSA's Pipeline Security Guidelines and it should be allowed to build upon these on-going efforts.

This hearing provides a great opportunity to discuss the work of both Government and the private sector to ensure all modes of transportation are secure from cyber threats and I look forward to a very productive conversation.

[The statement of Chairman Correa follows:]

STATEMENT OF CHAIRMAN J. LUIS CORREA

FEBRUARY 26, 2019

We have a great panel of distinguished Members on both sides of the aisle, and I look forward to working with you all to tackle the security challenges facing the transportation and maritime sectors. I am glad to hold our first hearing jointly with the Cybersecurity Subcommittee and its leaders, Chairman Richmond and Ranking Member Katko. I am also happy to welcome our two panels of witnesses today. We look forward to your testimony.

We are here today to discuss an important topic: The cybersecurity of our Nation's mass transit, rail, pipeline, and other surface transportation systems. Cyber threats

are a growing concern for security experts across many sectors—and the surface transportation sector is no different. Millions of Americans rely on surface transportation every day for critical services, and an attack against a large subway system or pipeline could have a hugely negative impact.

Government and industry have both struggled to address cyber threats, which are evolving quickly and becoming more complex. However, I believe DHS is well-positioned to lead cybersecurity efforts across critical infrastructure sectors, including the surface transportation sector.

Last year, Congress established the Cybersecurity and Infrastructure Security Agency, or CISA, making clear its status as the preeminent cybersecurity agency within the Federal Government. To secure surface transportation from cyber attacks, CISA works closely with TSA, which is responsible for securing all modes of transportation.

In December 2018, working with CISA, TSA released a Cybersecurity Roadmap, which sets priorities for securing transportation from cyber threats. The publication of this roadmap is an important step in addressing the cybersecurity of transportation, but it must be followed by concrete action.

In the surface mode, TSA works collaboratively with the system owners and operators who provide front-line security at the local level. In coordination with CISA, TSA must ensure owners and operators have access to the resources, intelligence, guidelines, and assessments needed to ensure the cybersecurity of their systems.

Government and industry stakeholders together must also address supply chain security concerns. We must make sure that surface transportation systems are not made vulnerable to cyber espionage due to unchecked foreign manufacturing of subway cars or other infrastructure.

Finally, some have questioned whether DHS has paid enough attention to pipeline security and have raised the idea of moving responsibility for securing pipelines to another department. Doing so would be foolhardy and go against the reasons Congress established DHS, TSA, and CISA. Only DHS has the scope of authorities and access to intelligence needed to address cyber threats across critical infrastructure sectors.

For example, only TSA has authority to issue Security Directives to require immediate implementation of security measures across or within modes of transportation in the face of an imminent threat or on-going attack.

DHS has made significant progress in securing pipelines, including recent updates to TSA's Pipeline Security Guidelines, and it should be allowed to build upon its on-going efforts.

This hearing provides a great opportunity to discuss the work of both Government and private industry to secure all modes of transportation from cyber threats, and I look forward to a productive conversation.

Mr. CORREA. Now I would like to recognize the Ranking Member of the subcommittee, the gentlewoman from Arizona, Mrs. Lesko, for an opening statement.

Mrs. LESKO. Thank you, Mr. Chairman.

Thank you to all of you that are here today including the people coming as our testifiers.

First, I would like to ask people to keep Representative Katko, in your prayers because his father passed away and that is why he is not here today and so Mr. Chairman, I do ask for unanimous consent for Representative Katko's statement to be added to the record.

Mr. CORREA. Without objection.

[The statement of Ranking Member Katko follows:]

STATEMENT OF RANKING MEMBER JOHN KATKO

Thank you, Mr. Chairman, and thank you for holding a hearing on this important issue.

I am pleased that my first subcommittee hearing as Ranking Member of the Cybersecurity, Infrastructure Protection, and Innovation subcommittee is a joint hearing with the subcommittee I was honored to chair for 4 years.

Our world is increasingly connected. Our phones, computers, cars, and televisions are only some of the things we use every day that are vulnerable to a cyber attack that causes disruptions.

But what about those objects that affect our everyday life, that we either don't see or don't consider them to be vulnerable to cyber attacks like pipelines that undergird this country's energy sector or the metro cars we rely on to get us around?

A cyber attack on the industrial control systems for our operational technology could wreak havoc across our Nation. It is an attack vector that we must take seriously and work to secure these technologies from motivated attackers.

Fortunately, we have two partners who are well-equipped to address these vulnerabilities. TSA brings the expertise about our pipelines and mass transit systems while CISA is the cyber expert. I want to reiterate what my colleague, Ranking Member Lesko said in her opening statement—TSA and CISA are stronger because of their ability to work together. Their value is made greater by the wealth of resources within DHS to help surface transportation operators be prepared for the cyber threats.

As a committee, we must be vigilant in making sure the various sectors of our economy are protecting their assets from physical and cyber harm. We cannot allow for those technologies that are foundational to our livelihood be a tool for a bad actor to launch a cyber attack.

Thank you to our witnesses for taking the time this morning to speak on this topic. I look forward to hearing from you.

Mrs. LESKO. Thank you, Mr. Chairman, and thank you for holding a hearing today on this very important topic.

TSA has security authorities over America's surface transportation modes including 6,700 mass transit systems, passenger and freight rail as well as motor coach in both rural and urban communities. In addition, pipelines are considered a mode of surface transportation for natural gas and hazardous materials. Across the United States, including in my home State of Arizona, TSA is responsible for securing more than 2½ million miles of pipelines carrying natural gas and other materials that quite literally fuel our economy.

While much progress has been made to provide better physical security for surface transportation, there remains growing concerns surrounding the cybersecurity of our Nation's surface transportation assets. As cyber actors become more sophisticated and surface transportation systems become increasingly reliant on computer systems, the vulnerability of this critical sector grows along with the risks posed by nefarious actors who may seek to exploit cybersecurity vulnerabilities to cause service disruptions or conduct economic espionage.

In general, surface transportation systems utilize a number of interconnected information systems that, when exposed, present cybersecurity vulnerabilities. According to the American Public Transit Association, cyber attacks against surface transportation operators can destroy an agency's physical systems, render them inoperable, hand over control of systems to an outside entity, or threaten the privacy of individuals or customers.

In the 115th Congress, the Republican Majority worked in a bipartisan manner to enact the TSA Modernization Act, the first-ever authorization of TSA since the agency was created in 2001. We also enacted the Cybersecurity and Infrastructure Security Agency Act of 2018 which created CISA in order to reform critical security programs within the Department and better equip DHS to support the cybersecurity of transportation systems.

Additionally, TSA Administrator Pekoske has worked to restructure the agency to reflect evolving mission needs. It is important to note that while threats against our transportation sector may be evolving, they are not diminishing. Legitimate concerns have been

raised as to the ability of TSA to provide necessary security for surface transportation assets and particularly pipelines.

While I believe TSA is best positioned as the Government's authority on transportation security, it is incumbent upon the agency to demonstrate its commitment to securing all modes of transportation. The Department of Homeland Security and its components must work to mitigate growing cybersecurity threats and work hand-in-hand with industry partners to promote a culture of security and keep America's economy fueled and moving with the public's confidence.

I do look forward to hearing the testimony before us today and thank you for being here.

I yield back, Mr. Chairman.

[The statement of Ranking Member Lesko follows:]

STATEMENT OF RANKING MEMBER DEBBIE LESKO

FEBRUARY 26, 2019

TSA has security authorities over America's surface transportation modes, including 6,700 mass transit systems, passenger and freight rail, as well as motorcoach, in both rural and urban communities. In addition, pipelines are considered a mode of surface transportation for natural gas and hazardous materials. Across the United States, including in my home State of Arizona, TSA is responsible for securing more than 2.5 million miles of pipelines carrying natural gas and other materials that quite literally fuel our economy.

While much progress has been made to provide better physical security for surface transportation there remains growing concern surrounding the cybersecurity of our Nation's surface transportation assets.

As cyber actors become more sophisticated and surface transportation systems become increasingly reliant on computer systems, the vulnerability of this critical sector grows, along with the risk posed by nefarious actors who may seek to exploit cybersecurity vulnerabilities to cause service disruptions or conduct economic espionage.

In general, surface transportation systems utilize a number of interconnected information systems that, when exposed, present cybersecurity vulnerabilities. According to the American Public Transit Association, cyber attacks against surface transportation operators can destroy an agency's physical systems, render them inoperable, hand over control of systems to an outside entity or threaten the privacy of individuals or customers.

In the 115th Congress, the Republican Majority worked in a bipartisan manner to enact the TSA Modernization Act, the first-ever authorization of TSA since the agency was created in 2001. We also enacted the Cybersecurity and Infrastructure Security Agency Act of 2018, which created CISA in order to reform critical security programs within the Department and better equip DHS to support the cybersecurity of transportation systems. Additionally, TSA Administrator Pekoske has worked to restructure the agency to reflect evolving mission needs.

It is important to note that while threats against our transportation sector may be evolving, they are not diminishing. Legitimate concerns have been raised as to the ability of TSA to provide necessary security for surface transportation assets, in particular pipelines. While I believe TSA is best positioned as the Government's authority on transportation security, it is incumbent upon the agency to demonstrate its commitment to securing all modes of transportation. The Department of Homeland Security and its components must work to mitigate growing cybersecurity threats and work hand-in-hand with industry partners to promote a culture of security and keep America's economy fueled and moving with the public's confidence.

Mr. CORREA. Thank you very much.

I will—I would like to recognize the Chair of the Committee on Homeland Security, Mr. Bennie Thompson, for some opening remarks, sir.

Mr. THOMPSON. Thank you very much, Chairman Correa; Ranking Member Lesko, on your maiden voyage as Ranking Member, welcome.

I would also like to express my sympathies to Ranking Member Katko on the loss of his father.

But also, this hearing today is very important, the cyber threats facing the U.S. surface transportation sector. Since the 9/11 attacks, the U.S. Government has focused on closing gaps in physical aviation security by Federalizing passenger and baggage screening, hardening cockpit doors, and deploying improved screening technologies and training.

In September 2018 the subcommittees held a joint hearing highlighting the potential harm from important undisclosed vector cyber threats in aviation. Today we will provide the same attention to cybersecurity threats to the surface transportation sector.

With TSA dedicating most of its resources to protecting aviation, the surface transportation sector including freight and passenger trains, commuter rails, mass transit, buses, and pipelines presents relatively a soft target for mass casualty attacks. We rely on these diverse assets not only for our shipping and other transports of natural gas, and a host of other activities essential to the health of our economy and National security.

In recent years, surface transportation systems overseas have been hit by terrorist attacks. On our own shores, New York City's subway was a target of a failed terrorist plot in December 2017. Given the level of risk to surface transportation, I am concerned that we have not sufficiently protected this sector against cyber threats.

To date no cyber attacks have disrupted the actual operations of surface transportation systems but attacks have resulted in financial disruption and affected public confidence in various modes of surface transportation. These small-scale attacks have shown that a relatively simple intrusion could up end surface transportation services causing significant harm and disruption.

Last year Congress established Cybersecurity and Infrastructure Security Agency or CISA as the operational agency within the Federal Government [inaudible] on cybersecurity information sharing. CISA will continue to play a critical role in providing cybersecurity resources within DHS including to TSA and to industries, to combat cyber threats to critical infrastructure. TSA for its part maintains responsibility for the security of all modes of transportation. Working together within DHS, CISA and TSA are uniquely positioned to address cyber threats in transportation.

I would note that DHS's authorities and capabilities across critical infrastructures' sectors in all modes of transportation makes it better positioned to secure pipelines than the Department of Energy, despite some suggestions to the contrary.

In December 2018, in coordination with CISA, TSA released its first-ever Cybersecurity Roadmap, providing a vision for the future of cybersecurity across all modes of transportation, while DHS is headed in the right direction much work remains. In many cases surface transportation sector-owners and -operators struggle with the same cyber challenges that plague other industries: A National shortage of skilled cybersecurity personnel; a work force with mini-

mal cybersecurity training and awareness; and resource constraints across the board.

Finally, at a hearing on surface transportation security, I would be remiss if I did not point out that TSA remains non-compliant with requirements to publish surface transportation security regulations which were enacted over a decade ago in the Implementation Recommendations of the 9/11 Commission Act of 2007.

I would like to at some point, Mr. Chairman, hope to get a response to why we have not had that take place.

With that I yield back.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

FEBRUARY 26, 2019

Since the 9/11 attacks, the U.S. Government has focused on closing gaps in physical aviation security by Federalizing passenger and baggage screening, hardening cockpit doors, and deploying improved screening technologies and training.

In September 2018, the subcommittees held a joint hearing highlighting the potential harm from an important, underdiscussed vector: Cyber threats to aviation. Today, we will provide the same attention to cybersecurity threats to the surface transportation sector.

With TSA dedicating most of its resources to protecting aviation, the surface transportation sector—including freight and passenger trains, commuter rail, mass transit, buses, and pipelines—presents a relatively soft target for mass-casualty attacks. We rely on these diverse assets not only support for our personal and business travel, but also commercial shipping, the transport of natural gas, and a host of other activities essential to the health of our economy and National security.

In recent years, surface transportation systems overseas have been hit by terrorist attacks. On our own shores, New York City's subway was the target of a failed terrorist plot in December 2017. Given the level of risk to surface transportation, I am concerned that we have not sufficiently protected this sector against cyber threats.

To date, no cyber attacks have disrupted the actual operations of surface transportation systems, but attacks have resulted in financial disruption and affected public confidence in various modes of surface transportation. These small-scale attacks have shown that a relatively simple intrusion could upend surface transportation services, causing significant harm and disruption.

Last year, Congress established Cybersecurity and Infrastructure Security Agency, or CISA, as the operational agency within the Federal Government charged with serving as the primary civilian interface for cybersecurity information sharing. CISA will continue to play a critical role in providing cybersecurity resources within DHS, including to TSA, and to industry to combat cyber threats to critical infrastructure.

TSA, for its part, maintains responsibility for the security of all modes of transportation.

Working together within DHS, CISA, and TSA are uniquely positioned to address cyber threats to transportation.

I would note that DHS's authorities and capabilities across all critical infrastructure sectors and all modes of transportation makes it better positioned to secure pipelines than the Department of Energy, despite some suggestions to the contrary.

In December 2018, in coordination with CISA, TSA released its first-ever Cybersecurity Roadmap, providing a vision for the future of cybersecurity across all modes of transportation.

While DHS is headed in the right direction, much work remains. In many cases, surface transportation sector owners and operators struggle with the same cyber challenges that plague other industries: A National shortage of skilled cybersecurity personnel, a workforce with minimal cybersecurity training and awareness, and resource constraints across the board.

Owners and operators must also address supply chain concerns, including those posed by the emergence of a Chinese state-owned enterprise manufacturing subway cars for U.S. mass transit systems. Government and industry must work together to ensure that cyber threats and vulnerabilities are fully understood and appropriately addressed.

Finally, at a hearing on surface transportation security, I would be remiss if I did not point out that TSA remains non-compliant with requirements to publish surface

transportation security regulations, which were enacted over a decade ago in the Implementing Recommendations of the 9/11 Commission Act of 2007.

The rules required under the law would help TSA to better assess and address vulnerabilities within the surface transportation sector, including cybersecurity vulnerabilities.

I look forward to hearing from this panel of witnesses today, and I hope they will give us a candid assessment of the cybersecurity posture of our surface transportation sector.

Mr. CORREA. Thank you, Chairman Thompson, for those opening statements.

Now I would like to recognize the co-Chair of this hearing today, Mr. Richmond, Chairman of the Cybersecurity, Infrastructure Protection, and Innovation Subcommittee for an opening statement. Welcome, sir.

Mr. RICHMOND. Thank you, Mr. Chairman.

I will recognize the Chairman of the whole—full committee, Mr. Bennie Thompson, from Mississippi.

I will also join my colleagues in extending my condolences to Congressman Katko. As a person who has lost two fathers, I understand what he is going through and we wish him the best.

I want to start by congratulating Congressman Correa, on becoming Chairman of the Transportation and Maritime Security Subcommittee. I look forward to working with you to improve the cybersecurity posture of our transportation infrastructure.

Last fall our subcommittees held a joint hearing to assess cybersecurity risks to aviation. We learned that cyber threats to aviation are persistent, that cyber tools can be used to engage in cyber espionage or undermine confidence in the aviation industry and that the safety of air travelers requires us to stay a step ahead of bad actors.

In short, we learned that cybersecurity posture of the aviation sector is a National security, economic security, and public safety imperative. The same can be said for the cybersecurity posture of our surface transportation systems. Surface transportation includes roads, rail, maritime facilities, and pipelines and my district is rich in all of them so I am glad that we are beginning the 116th Congress with this hearing.

Compared to the aviation sector, surface transportation receives relatively little in Federal funding to support security. Outside of the Transit Security Grant Program which is awarded to public transportation entities and primarily used to secure against physical threats, surface transportation owners and operators foot the bill for security themselves.

But the Federal Government is not off the hook, it plays a critical role in providing the situational awareness, security assessments, and guidance to stakeholders that inform surface transportation security investments.

In a decade-and-a-half since it was established, the Department of Homeland Security has matured its ability to convene stakeholders, leverage its cross-component expertise, and share actionable intelligence analysis and guidance to help address pressing National security challenges.

Whether or not the Federal Government can effectively partner with stakeholders to secure surface transportation modes from cyber attacks, rests on DHS's ability to continue to perform and

build on these capabilities. Approximately 125,000 miles of pipelines valued at 1.9 billion move oil and gas through Louisiana every day. The industry employs over 2,500 people in the State; toward that end I was pleased that the Pipeline Cybersecurity Initiative was one of the first priorities announced by the new National Risk Management Center last year and updated Pipeline Security Guidelines were finally released last March.

I am encouraged that the Department is redoubling its efforts to improve the cybersecurity of pipelines by enhancing the in-house collaboration between CISA and TSA, and engaging with the private sector.

I believe the Pipeline Security Initiative has the potential to provide a more comprehensive understanding of the unique cybersecurity risks to pipelines, particularly as the sector relies more on the industrial internet of things; that knowledge will empower stakeholders to address cybersecurity risks more strategically. Although the Initiative was first announced as one of the NRMC's initial sprint, I hope that it will evolve into a more permanent collaboration.

I am concerned however that the updated Pipeline Security Guidelines do not address supply chain risk management; moreover I would be interested to know how TSA is implementing the 10 recommendations the Government Accountability Office made in December related to its management of Pipeline Security Program. The safety of my community and the economy of my district depends on DHS getting this mission right.

I would be remiss if I did not also raise my concerns about the cybersecurity posture of both passenger and freight rail, particularly as passenger rail cars incorporate automatic train control, network and train-line control and monitoring and diagnostics, among other technologies.

Last month I read a troubling report of a Chinese rail company significantly under-bidding competitors to win transit rail contracts in four major markets. I am aware of China's political and economic ambitions. The intelligence community and Congress have been clear in cautioning against the use of Chinese telecommunications products.

But it is unclear to me whether the Federal Government has assessed what, if any additional cybersecurity threat is posed by contracting with a Chinese company to purchase railcars with advanced technologies. It is also unclear whether the Federal Government is providing any guidance to local transit authorities to ensure cybersecurity is incorporated into their procurement process.

I look forward to discussing these issues with the witnesses today and I yield back the balance of my time.

[The prepared statement of Chairman Richmond follows:]

STATEMENT OF CHAIRMAN CEDRIC RICHMOND

FEBRUARY 26, 2019

Last fall, our subcommittees held a joint hearing to assess cybersecurity risks to aviation. We learned that cyber threats to aviation are persistent, that cyber tools can be used to engage in cyber espionage or undermine confidence in the aviation industry, and that the safety of air travelers requires us to stay a step ahead of bad actors.

In short, we learned that the cybersecurity posture of the aviation sector is a National security, economic security, and public safety imperative. The same can be said for the cybersecurity posture of our surface transportation systems.

Surface transportation includes roads, rail, maritime facilities, and pipelines, and my district is rich in all of them, so I'm glad we are beginning the 116th Congress with this hearing. Compared to the aviation sector, surface transportation receives relatively little in Federal funding to support security.

Outside of the Transit Security Grant Program—which is awarded to public transportation entities and primarily used to secure against physical threats—surface transportation owners and operators foot the bill for security themselves.

But the Federal Government is not off the hook. It plays a critical role in providing the situational awareness, security assessments, and guidance to stakeholders that inform surface transportation security investments.

In the decade-and-a-half since it was established, the Department of Homeland Security has matured its ability to convene stakeholders, leverage its cross-component expertise, and share actionable intelligence analysis and guidance to help address pressing National security challenges.

Whether or not the Federal Government can effectively partner with stakeholders to secure surface transportation modes from cyber attacks rests on DHS's ability to continue to perform and build on these capabilities.

Approximately 125,000 miles of pipelines—valued at $1.9 billion—move oil and gas through Louisiana every day. The industry employs over 2,500 people in the State. Toward that end, I was pleased that the Pipeline Cybersecurity Initiative was one of the first priorities announced by the new National Risk Management Center last year and the updated Pipeline Security Guidelines were finally released last March. I am encouraged that the Department is redoubling its efforts to improve the cybersecurity of pipelines by enhancing the in-house collaboration between CISA and TSA and engaging with the private sector.

I believe the Pipeline Cybersecurity Initiative has the potential to provide a more comprehensive understanding of the unique cybersecurity risks to pipelines, particularly as the sector relies more on the industrial internet of things. That knowledge will empower stakeholders to address cybersecurity risks more strategically. Although the Initiative was first announced as one of the NRMC's initial "sprint," I hope that it will evolve into a more permanent collaboration. I am concerned, however, that the updated Pipeline Security Guidelines do not address supply chain risk management.

Moreover, I will be interested to know how TSA is implementing the 10 recommendations the Government Accountability Office made in December related to its management of the Pipeline Security Program. The safety of my community and the economy of my district depend on DHS getting this mission right.

I would be remiss if I did not also raise my concerns about the cybersecurity posture of both passenger and freight rail, particularly as passenger rail cars incorporate automatic train control, network and trainline control, and monitoring and diagnostics, among other technologies. Last month, I read troubling reports of a Chinese rail company significantly underbidding competitors to win transit rail contracts in four major markets.

I am aware of China's political and economic ambitions. The intelligence community and Congress have been clear in cautioning against the use of Chinese telecommunications products.

But it is unclear to me whether the Federal Government has assessed what, if any, additional cybersecurity threat is posed by contracting with a Chinese company to purchase rail cars with advanced technologies.

It is also unclear whether the Federal Government is providing any guidance to local transit authorities to ensure cybersecurity is incorporated into their procurement processes.

I look forward to discussing these issues with the witnesses and I yield back the balance of my time.

Mr. CORREA. Thank you, Chairman Richmond. I also would like to congratulate you on your Chairmanship; I look forward to working with you as well.

Other Members of the subcommittee are reminded that under the committee rules, opening statements may be submitted for the record.

[The statement of Honorable Jackson Lee follows:]

STATEMENT OF HONORABLE SHEILA JACKSON LEE

Good morning Chairman Correa and Chairman Richmond, Ranking Member Lesko and Ranking Member Katko, for convening today's joint hearing on "Securing U.S. Surface Transportation From Cyber Attacks."

At the outset, let me congratulate Chairman Correa and Chairman Richmond on your elections to lead the Homeland Security Subcommittees on Transportation and Maritime Security and Cybersecurity, Infrastructure Protection and Innovation Committee, respectively.

I look forward to continuing to work with each of you along with returning Members of the committee and welcome an outstanding group of new Members on both sides of the aisle, whom I trust will find the important work advanced by this committee as fulfilling and rewarding as I have since joining it as its inception.

Today's witnesses:

Panel I

- Mr. Bob Kolasky, director, National Risk Management Center, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security;
- Sonya T. Proctor, director, Surface Division, Office of Security Policy and Industry Engagement, Transportation Security Administration.

Panel II

- Ms. Rebecca Gagliostro, director, security, reliability, and resilience, Interstate Natural Gas Association of America;
- James A. Lewis, senior vice president, Center for Strategic and International Studies;
- Erik Robert Olson, vice president, Rail Security Alliance;
- Mr. John Hultquist, director of intelligence analysis, FireEye (Minority witness).

I thank each of today's witnesses for bringing their expert view on the state of cybersecurity and surface transportation in the United States.

I note that several of today's witnesses warn about China and the security of transportation systems in the United States.

Their concern is shared by the Department of Defense in its annual report to Congress: Military and Security Developments Involving the People's Republic of China 2018.

The report states that China obtains foreign technology through imports, foreign direct investment, industrial and cyber espionage, and establishment of foreign research and development (R&D) centers.

In addition, an assessment of Cyber Operations by DoD said that People's Liberation Army researchers believe that building strong cyber capabilities is necessary to protect Chinese networks and advocate seizing "cyber space superiority" by using offensive cyber operations to deter or degrade an adversary's ability to conduct military operations against China.

These findings by the DoD give our committee ample reason to consider the cybersecurity implications of China's activity in the transportation sector.

The Transportation Security Administration (TSA) is responsible for both the physical security and cybersecurity of all modes of transportation, including pipelines.

In November 2018, TSA released the "TSA Cybersecurity Roadmap for 2018," its first-ever cybersecurity roadmap.

The Roadmap will guide TSA's oversight of the cybersecurity of the transportation systems sector over the next 5 years by focusing on four priority areas, which include risk identification, vulnerability reduction, consequence mitigation, and enabling cybersecurity outcomes.

In addition, the Roadmap emphasizes TSA's commitment to recruiting, retaining, and training technical and cyber talent to improve its ability to engage with stakeholders on cybersecurity and information technology issues.

Finally, the Roadmap highlights TSA's collaboration with the Cybersecurity and Infrastructure Security Agency (CISA), which is the operational component within DHS charged with serving as the primary Federal civilian interface for cybersecurity information sharing.

We know the threats that computing devices and systems face, which are almost too numerous to count:

- Bot-nets;
- Ransomware;
- Zero Day Events;
- Malware;
- Denial-of-Service Attacks;

- Distributed Denial-of-Service Attacks;
- Pharming;
- Phishing;
- Data Theft;
- Data Breaches;
- SQL Injection;
- Man-in-the-Middle Attack.

The list goes on, but suffice to say that as hard as any one person in our Government is working to stop cyber attacks there are likely another thousand attempting to breach a system or device or technology used by a United States citizen.

Vulnerabilities of computing systems are not limited to intentional attacks, but can include acts of nature, human error, or technology failing to perform as intended.

I am particularly concerned about cybersecurity of transportation for pipelines, bridges, tolls, air traffic control systems, commercial aircraft, ports, and automobiles.

Government agencies and political institutions around the world have acknowledged that air traffic management and control (ATM/ATC) vulnerabilities could be used to undermine National security.

Any breach of the U.S. air traffic control system can lead to flight interruptions that may result in cancellations.

The number, type, and severity of cyber threats experienced by ports, service providers, or port customers are unknown because victims generally prefer not to report incidents and to pay or absorb costs resulting from breaches or thefts.

Another reason for underreporting is that companies and ports often are unaware that their cybersecurity has been breached.

In January 2019, the American Association of Port Authorities (AAPA) identified nearly $4 billion in crucial port and supply chain security needs over the next 10 years.

The AAPA says that funding is needed to ensure America's port facilities are properly equipped to address new and evolving security challenges.

The report recommends refocusing the Federal Emergency Management Agency's Port Security Grant Program to better meet the security infrastructure needs of publicly-owned commercial seaports and related maritime operations.

AAPA recommends funding an estimated $2.62 billion in maintenance and upgrades to port security equipment and systems, and another $1.27 billion for investments to tackle cybersecurity, active shooter, drone mitigation, resiliency, and other evolving security threats.

It is reported that the U.S. Government invests $100 million annually in the Port Security Grant Program.

This grant program began after 9/11, and it is estimated that by the end of 2017, container volumes through U.S. ports have increased 71 percent and total foreign trade tonnage had increased 37 percent, while cruise passenger traffic nearly doubled by the end of 2018.

During this time, 85 percent of AAPA U.S. member ports report that they anticipate direct cyber or physical threats to their ports to increase over the next 10 years.

The 2017 APM Maersk cyber attack illustrates how an incident can start outside the United States and have a cascading impact on ports and terminal operations across the globe.

Further evidence on the cyber vulnerability of ports, comes from October 15, 2014, in a report by CyberKeel entitled, "Maritime Cyber-Risks," which focused on financial thefts; alteration of carrier information regarding cargo location; barcode scanners used as hacking devices (a variation of the light bulb vulnerability described above); targeting of shipbuilding and maritime operations; cyber-enabled large drug smuggling operations; compromising of Australian customs and border protection; spoofing a vessel Automated Identification System (AIS); drilling rig cyber attack; vessel navigation control hack; GPS jamming; vulnerabilities in the Electronic Chart Display and Information System; and a Danish Maritime Authority breach.

In 2015, I hosted a briefing on "Cyber Security Threat Posed by the Ability to Hack Automobiles," which provided information on the growing threat of remote attacks against moving vehicles and the privacy of consumer data captured by automotive systems.

Finally, the use of untrustworthiness of transportation infrastructure can have significant impacts on our Nation's economy.

An important part of cybersecurity is establishing and maintaining a cybersecurity culture both within the Federal Government and throughout the private sector.

We must change the way we perceive and respond to cybersecurity vulnerabilities and threats.

We must be steadfast in our resolve to protect the Nation's transportation system from cyber threats.

I look forward to the testimony of today's witnesses.

Thank you.

Mr. CORREA. With that being said I welcome the first panel of witnesses.

Our first witness is Mr. Bob Kolasky, who serves as director of the National Risk Management Center at the Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security. As director he oversees the Center's efforts to facilitate strategic cross-sector risk management approach to cyber and physical threats to our critical infrastructure.

Next we will have Ms. Sonya Proctor, who serves as director of the Surface Division within the Office of Security Policy or OSP, at the Transportation Security Agency. Ms. Proctor's responsibilities include developing risk-based and effective security policy in collaboration with stakeholders in surface transportation modes.

Without objection, the witnesses' full statements will be inserted into the record and I will ask each witness to summarize his or her statements in 5 minutes, beginning with Mr. Kolasky.

Welcome, sir.

STATEMENT OF ROBERT KOLASKY, DIRECTOR, NATIONAL RISK MANAGEMENT CENTER, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. KOLASKY. Thank you, Chairman.

Chairman Correa, Chairman Thompson, Chairman Richmond, Ranking Member Lesko, and Members of the subcommittee, good morning and thank you for the opportunity to testify regarding the Department's on-going and collaborative efforts to strengthen the cybersecurity of our Nation.

Today, as the subject of the hearing, I will focus my remarks on surface transportation including pipelines, mass transit, freight, rail, and our highways.

First however I do want to thank the committee for its leadership in establishing the Cybersecurity and Infrastructure Security Agency, CISA. By creating our new agency in law, Congress formally recognized DHS's role as the leader of the National effort to safeguard Federal networks and critical infrastructure from cyber and physical threats.

CISA delivers organization-specific and cross-sector risk management support to enhance the resiliency of our Nation's critical infrastructure. We are the main Federal interface for sharing cyber-threat indicators. We provide a broad range of cybersecurity threat detector response and coordination capabilities to assist industry across all sectors, including surface transportation, for securing their operations. Our capabilities bring together the intelligence committee, law enforcement, international partners, and the private sector.

As part of CISA, I serve as the director of the National Risk Management Center. The Center brings together industry and Government for collaborative planning, analysis, and prioritization in

order to reduce risk to critical infrastructure. These efforts complement and support the day-to-day operations across our agency and are intended to focus on the most significant risks facing the Nation's critical infrastructure. To that end cyber threats remain one of the most significant strategic risks for the United States.

Critical infrastructure cyber incidents however are rarely sector-specific which means we can't afford to take a sector-specific approach to risk management. Our adversaries target common vulnerabilities in systems across sectors. They target companies in one sector to launch attacks on a [inaudible] the growing interdependencies across sectors demand an integrated approach.

An attack on the transportation sector has operational impact and transcends the operations across the transportation sector. That is one reason why we did establish the National Risk Management Center. Planning, operations, and information sharing to secure critical infrastructure must not be stovepiped; this is because of the global, borderless, interconnected nature of cyber space where strategic threats can manifest in the homeland without advance warning and speed of collaboration is essential.

In the coming months the National Risk Management Center will finalize the identification of a set of National Critical Functions. National Critical Functions are defined as the functions of Government and the private sector, so vital to the United States that their disruption, corruption, or dysfunction could have a debilitating impact on National security, economic security, National public health, or safety, and we identified these in partnership with industry and our colleagues across the Government.

Through this process we have already identified functions associated with surface transportation such as the movement of commodities through pipelines and the generation of electricity that need to be prioritized. Because of that last year as you all mentioned, we launched the Pipeline Security Initiative to build upon past work in the sector.

This effort is a partnership between CISA, TSA, the Department of Energy, as well as industry. CISA is coordinating risk management planning and tasking its cybersecurity operations, provide technical capabilities in support of my colleague Sonya and her team as the sector-specific agency. TSA's relationship with the sector and understanding of pipeline operations is critical to the success of this initiative.

The Pipeline Security Initiative is conducting cybersecurity assessments on pipelines to identify and mitigate vulnerabilities. The first comprehensive assessment was completed in December 2018 and we expect to do 9 more this year. These are some of the most comprehensive, in-depth, cyber assessments the U.S. Government has done on pipelines to date. Based on these assessments the NRMC will be conducting initial analysis of how best to reduce risk to the Nation's pipeline infrastructure, working with industry to prioritize mitigation activities.

Another example of our work to support the transportation sector is industrial control security. Much of our Nation's surface transportation is dependent on industrial control systems to monitor, control, and safeguard operation. We at CISA have a long history of working to provide technical expertise and to share information

with ICS vendors and we will continue to do that with a focus on surface transportation.

The final area I want to talk about, the National Risk Management Center's efforts are our efforts around supply chain security. To address supply chain risks CISA has established an Information and Communications Technology Supply Chain Risk Management Task Force. This is a public-private partnership to facilitate mitigation of emerging supply chain threats.

Work is on-going on 4 separate work streams intended to improve threat information, better understand priority Supply Chain risks, and incentivize and enhance Supply Chain Risk Management. This work will help transportation sectors as well as critical infrastructure and Federal networks.

In closing, CISA will continue to be a partner to our Government and industry colleagues with the twin imperative of addressing the cyber threats we see today and shaping the risk environment of tomorrow. I am convinced that such an approach will leave us better prepared to address any challenges we face from our adversaries now and in the future.

Once again thank you for the opportunity to appear before the subcommittee today. I look forward to your questions.

[The prepared statement of Mr. Kolasky follows:]

PREPARED STATEMENT OF ROBERT KOLASKY

FEBRUARY 26, 2019

Chairman Richmond, Chairman Correa, Ranking Member Katko, Ranking Member Lesko, and Members of the subcommittees, thank you for the opportunity to testify regarding the U.S. Department of Homeland Security's (DHS) on-going efforts to reduce and mitigate risks to our Nation's critical infrastructure. I have the privilege of serving as the director of the National Risk Management Center (NRMC) at the Cybersecurity and Infrastructure Security Agency (CISA). The NRMC operates as a planning, analysis, and collaboration center bringing together industry and multiple parts of Government to identify, analyze, prioritize, and reduce risks to critical infrastructure. The NRMC's efforts are centered on the "secure tomorrow" mantle of CISA's mission—complementing and drawing from the day-to-day information sharing, technical analysis, and operational assistance missions from elsewhere in the agency.

My testimony today will focus on the cybersecurity of surface transportation systems, including pipelines, mass transit systems, freight rail systems, and highways. Both CISA and the Transportation Security Administration (TSA) play a critical role in accomplishing this mission. CISA is leading National efforts to defend the Nation's critical infrastructure today and secure tomorrow by partnering with industry and Government to reduce risk from cyber, physical, and hybrid threats. Thanks to Congress's leadership and passage of the Cybersecurity and Infrastructure Security Agency Act of 2018 (Pub. L. 115–278), we are now even better poised to further the maturation of the organization to best reflect our essential mission and role in securing cyber space. CISA's efforts to secure surface transportation are carried out in close coordination with the TSA and Department of Transportation, the Sector-Specific Agencies (SSA) for the surface transportation portion of the Transportation Systems Sector.

CYBER THREATS

Cyber threats remain one of the most significant strategic risks for the United States, threatening our National security, economic prosperity, and public health and safety. The past several years have marked a growing awareness of the cyber domain in the public consciousness. We have seen advanced persistent threat actors, including hackers, cyber criminals, and nation-states, increase the frequency and sophistication of their attacks. Our adversaries have been developing and using advanced cyber capabilities in attempts to undermine critical infrastructure, target our

livelihoods and innovation, steal our National security secrets, and threaten our democratic institutions.

Cybersecurity threats affecting surface transportation have the potential to impact the industrial control systems that operate pipelines, mass transit, freight rail systems, and our highway infrastructure. For example, America depends heavily on the 2.7 million miles of pipeline crisscrossing our country. Increasingly, the business operations and control systems that are vital to the continuity of this part of our energy posture are threatened by cyber attacks from nation-states and other malicious actors. Many pipelines are now supplied with industrial control systems, automated pressure regulators, and control valves. If this pipeline infrastructure is intentionally attacked, control valves and pressure regulators could be affected. Failure of these technologies could lead to pressure surges causing emergency shutdowns, unexpected explosions and fires, and other serious consequences. The recently-published Worldwide Threat Assessment of the intelligence community states, "China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States."

Similarly, trains are now supplied with on-board information technology (IT) systems that provide and receive real-time updates on track conditions, train position, train separation, car status, and other operational data. While such technologies are designed to provide faster and more reliable communications, these wireless communication advances result in trains no longer functioning as closed systems, thus increasing the cyber risks.

Today's industrial control systems within highway infrastructure are often not only automated but highly integrated. Interconnected road networks are controlled by numerous systems and devices such as traffic signal systems, ramp metering systems, road weather information systems, and field devices that feed into a traffic management center. If an individual system or device was deliberately attacked, the potential to affect multiple control systems would be a distinct reality.

CYBERSECURITY PRIORITIES

CISA, our Government partners, and the private sector are all engaging in a more strategic and unified approach toward improving our Nation's overall defensive posture against malicious cyber activity. In May of last year, DHS published the Department-wide DHS Cybersecurity Strategy, outlining a strategic framework to execute our cybersecurity responsibilities during the next 5 years. Both the Strategy and Presidential Policy Directive 21—Critical Infrastructure Security and Resilience, emphasize that we must maintain an integrated approach to managing risk.

The National Cyber Strategy, released in September 2018, reiterates the criticality of collaboration and strengthens the Government's commitment to work in partnership with industry to combat cyber threats and secure our critical infrastructure. Together, the National Cyber Strategy and DHS Cybersecurity Strategy guide CISA's efforts to secure Federal networks and strengthen critical infrastructure. DHS works across Government and critical infrastructure industry partnerships to share timely and actionable information as well as to provide training and technical assistance. Our work enhances cyber threat information sharing between and among governments and businesses across the globe to stop cyber incidents before they occur and quickly recover when they do. By bringing together all levels of government, the private sector, international partners, and the public, we are enabling a collective defense against cybersecurity risks, while improving our whole-of-Government incident response capabilities, enhancing information sharing of best practices and cyber threats, strengthening our resilience, and facilitating safety.

CISA's National Cybersecurity and Communications Integration Center (NCCIC) provides entities with information, technical assistance, and guidance they can use to secure their networks, systems, assets, information, and data by reducing vulnerabilities, ensuring resilience to cyber incidents, and supporting their holistic risk management priorities. The NCCIC operates at the intersection of the Federal Government, State and local governments, the private sector, international partners, law enforcement, intelligence, and defense communities. The Cybersecurity Information Sharing Act of 2015 (Pub. L. 114–113) established DHS as the Federal Government's central hub for the sharing of cyber threat indicators and defensive measures. CISA's automated indicator sharing capability allows the Federal Government and private-sector network defenders to share technical information at machine speed.

Much of our Nation's surface transportation infrastructure is dependent on industrial control systems to monitor, control, and safeguard operational processes. Many of the industrial control systems currently in use were built for operability, effi-

ciency, and reliability during an era when security was a lower priority than it is today. CISA has a well-established history of working to secure industrial control systems across critical infrastructure. In 2004, DHS established the Control Systems Security Program to address growing concerns over the security of industrial control systems. Since 2009, DHS has maintained the Industrial Control Systems Joint Working Group as the primary body for communicating and partnering across all critical infrastructure sectors and the government at all levels to accelerate the design, development, and deployment of secure industrial control systems. CISA's industrial control systems cybersecurity capabilities include malware and vulnerability analysis; an operational watch floor to monitor, track, and investigate cyber incidents; incident response; international stakeholder coordination; and the creation and dissemination of threat briefings, security bulletins, and notices related to emerging threats and vulnerabilities impacting these technologies.

NATIONAL RISK MANAGEMENT

Our adversaries' capabilities on-line are outpacing our stove-piped defenses. Specifically, there has been a critical gap in cross-sector, cross-government coordination on critical infrastructure security and resilience. Working together with the private sector and other Government partners, we are taking collective action to strengthen cross-sector, cross-government coordination against malicious cyber actors.

Through the NRMC within CISA, we have stepped up our efforts to provide a comprehensive risk management approach to cyber and physical security. The NRMC is a core component of DHS's efforts to take a holistic cross-sector approach to managing risks to the critical functions that drive our economy and are necessary to our National security. Through the NRMC, Government and industry are coming together to create a more complete understanding of the complex perils that threaten the Nation's critical infrastructure.

Risk is increasingly cross-sector in nature. A siloed approach to risk identification and management simply will not work. By the nature of the threat, and infrastructure design, risk transcends infrastructure sectors, is shared across State and National lines, and is held by both Government and industry. As an example, we recently briefed industry on cyber activities that have been attributed to China. Attempts to steal intellectual property do not discriminate between sectors of our economy. From biotechnology, to aircraft components, to advanced rail equipment, and electrical generation equipment—information is at risk, and it can be weaponized. Similarly, the cascading nature of cyber incidents across sectors is very real. We need to look no further than NotPetya, the most costly cyber attack in history—which we have attributed to Russia—to see how risk easily jumps across sectors and continents and how it can hit private sector organizations particularly hard.

NATIONAL CRITICAL FUNCTIONS

Historically, the U.S. Government has focused on prioritizing critical infrastructure from the perspective of assets and organizations. A different approach for prioritization is needed to better address system-wide and cross-sector risks and dependencies. CISA, through the NRMC, is leading an effort to develop a set of National Critical Functions to guide critical infrastructure risk management.

National Critical Functions are defined as "the functions of Government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on National security, economic security, National public health or safety." This construct forces a risk management conversation that is less about whether an entity is a business or Government, and more about what an entity does to manage risk and what risk it enables. This framework allows us to look at issue sets in the risk management space not in isolation, but with a more holistic context.

We are partnering with SSAs and all 16 critical infrastructure sectors, including the Transportation Systems, Communications, Financial Services, and Energy sectors to identify and validate National Critical Functions. This list will be finalized in the coming months and will form the basis for subsequent analysis—including consequence modeling and dependency analysis—in order to develop a Risk Register of the most pressing threats facing the critical infrastructure community. Such a Risk Register will guide collective action between Government and industry on how to best address risk management.

In doing the critical functions work, we have already identified aspects associated with surface transportation, such as pipeline operations, that need to be prioritized in terms of security. Although we are in our early stages of that work, we agree with the committee on the pressing need to address risks associated with nation-state exploitation of vulnerabilities that link information to infrastructure oper-

ations and which could have significant consequences on community and economic security.

SURFACE TRANSPORTATION CYBERSECURITY

The Pipeline Security Initiative is a partnership between CISA, TSA, the Department of Energy, and industry. Bad actors have shown interest in infiltrating systems in sectors with less mature cyber hygiene, and using that access to better understand ways to manipulate equipment in sectors with more advanced security protocols. This can lead to critical pipeline systems, including water, natural gas, and liquid fuels, being at risk.

By leveraging the TSA's SSA expertise and CISA's technical cybersecurity capabilities, the Pipeline Security Initiative is working to improve our ability to identify and mitigate vulnerabilities to the pipeline ecosystem. This initiative uses different voluntary assessments—ranging from single and multi-day inspections to self-assessments—to help our industry partners identify and mitigate potential vulnerabilities and provide the Government with a broader view of pipeline security risk.

In December 2018, we completed our first comprehensive assessment under this new initiative. This initial assessment served as a successful test-bed to ensure that tools and other techniques offer the detail and data necessary to conduct the comprehensive analysis needed to ensure critical services and product flow through the pipeline systems. We anticipate 9 more assessments in 2019.

SUPPLY CHAIN RISKS

Information and communications technology (ICT) is critical to every business and Government agency's ability to carry out its mission efficiently and effectively. Vulnerabilities in ICT can be exploited intentionally or unintentionally through a variety of means, including deliberate mislabeling and counterfeits, unauthorized production, tampering, theft, and insertion of malicious software or hardware. If these risks are not detected and mitigated, the impact to the ICT could be a fundamental degradation of its confidentiality, integrity, or availability and potentially create adverse impacts to essential Government or critical infrastructure systems.

Increasingly sophisticated adversaries seek to steal, compromise, alter, or destroy sensitive information on systems and networks, and risks associated with ICT may be used to facilitate these activities. The Office of the Director of National Intelligence (ODNI) acknowledges that "the U.S. is under systemic assault by foreign intelligence entities who target the equipment, systems, and information used every day by Government, business, and individual citizens." The globalization of our supply chain can result in component parts, services, and manufacturing from sources distributed around the world. ODNI further states, "Our most capable adversaries can access this supply chain at multiple points, establishing advanced, persistent, and multifaceted subversion. Our adversaries are also able to use this complexity to obfuscate their efforts to penetrate sensitive research and development programs, steal intellectual property and personally identifiable information, insert malware into critical components, and mask foreign ownership, control, and/or influence of key providers of components and services."

CISA has launched the ICT Supply Chain Risk Management (SCRM) Task Force as a public-private partnership to mitigate emerging supply chain threats. The Task Force is the main private-sector point of entry for our SCRM efforts and is jointly chaired by DHS and the chairs of IT and Communications Sector Coordinating Councils. The Task Force is focused on supply chain threat information sharing, supply chain threat mapping and assessment, establishing criteria for qualified bidder and manufacturer lists, and incentivizing the purchase of ICT from original manufacturers and authorized resellers.

CONCLUSION

In the face of increasingly sophisticated threats, DHS employees stand on the front lines of the Federal Government's efforts to defend our Nation's critical infrastructure from natural disasters, terrorism and adversarial threats, and technological risk such as those caused by cyber threats. The coming revolution of autonomous operations of infrastructure and other core functions, which combines data, machine learning, algorithms, and computing power and which is associated with massive new markets in artificial intelligence, smart cities, and quantum computing is going to radically change the nature of National security. The underpinning systems enabling functioning infrastructure have become more complex, and design considerations have created new vulnerabilities. Combine the reality of adversaries who are seeking to achieve strategic gain in the global marketplace and there is an

essential imperative to have security remain a first-order consideration for key infrastructure deployments and in the establishment of supply chains.

CISA is working with partners to meet this century's risks. Doing so requires being vigilant about security risk today and playing the long game—which will require continued collaboration between the Executive and Legislative branches. As the committee considers these issues, we are committed to working with Congress to ensure that this effort is done in a way that cultivates a safer, more secure, and resilient homeland.

Thank you for the opportunity to appear before the committee today, and I look forward to your questions.

Mr. CORREA. Thank you, Mr. Kolasky.

I will now recognize Ms. Proctor, for your testimony; if you can summarize your statements in 5 minutes. Thank you.

STATEMENT OF SONYA T. PROCTOR, DIRECTOR, SURFACE DIVISION, OFFICE OF THE SECURITY POLICY AND INDUSTRY ENGAGEMENT, TRANSPORTATION SECURITY ADMINISTRATION

Ms. PROCTOR. Thank you.

Good morning, Chairman Thompson, Chairman Correa, and Richmond, and Ranking Member Lesko, and distinguished Members of the subcommittee. Thank you for the opportunity to appear before you this morning to discuss the Transportation Security Administration's efforts to secure surface transportation systems including oil and natural gas pipelines from cybersecurity risks. I also want to thank you for the TSA Modernization Act and the support of that.

TSA is committed to securing the transportation sector, which includes pipelines, against evolving and emerging risks such as cyber attacks; partnering with our private-sector partners to secure surface transportation from cyber attacks is a critically important and complex undertaking.

The U.S. surface transportation system is a complex interconnected and largely open network comprised of mass transit systems, passenger and freight railroads, over-the-road bus operators, motor carrier operators, pipelines, and maritime facilities. The various modes that make up the system operate daily in close coordination with and proximity [inaudible] transportation system, operating securely and safely.

Every year more than 10 billion trips are taken on 6,800 U.S. mass transit systems which range from small bus-only systems in rural areas to large multi-modal systems in urban areas. Over-the-road bus operators carry approximately 604 million inter-city bus passengers each year; over 3,300 commercial bus companies travel on the 4 million miles of roadway in the United States and on more than 600,000 highway bridges and through over 470 tunnels. Those same roads, bridges, and tunnels support the movement of goods throughout the country by 8 million large-capacity commercial trucks.

As for our railroads and pipelines, more than 570 individual freight railroads carrying essential goods, operate on nearly 140,000 miles of track and 2.75 million miles of pipelines owned and operated by approximately 3,000 private companies, transporting natural gas, refined petroleum products, and other commercial products.

TSA's functions and authorities as a security agency are uniquely structured to tackle the challenges at the intersections of surface transportation and cyber risks. To secure these networks, TSA leverages its mature intelligence and analysis capability along with its vetting and credentialing programs to ensure it can quickly develop and promulgate risk mitigation guidelines and measures to effectively [inaudible] efforts are bolstered by strong partnerships, trust, and collaboration with our Federal industry and partners.

In this regard industry works with TSA to share their own unique vulnerabilities and security needs. Through this open communication we collaboratively develop programs and guidelines for industry to voluntarily adopt to increase their overall security posture an approach that has yielded significant security investments and improvements beyond what the agency would have achieved from a regulatory approach alone. We believe that this voluntary and collaborative approach to developing and implementing security measures has been successful.

However, we also recognize that should arise based on an eminent threat or real-world event the TSA administrator has unique authority to require immediate implementation of certain security measures through the issuance of security directives.

In December 2018 the TSA administrator issued the agency's Cybersecurity Roadmap which will guide efforts to prioritize cybersecurity measures within TSA and across the transportation system over the next 5 years. TSA approaches both cybersecurity and physical security by identifying, assessing, and mitigating the risk. TSA helps surface owners and operators identify vulnerabilities and risks in their operations and works with them to develop and implement risk mitigating solutions.

In closing TSA has been able to support the improvement of both physical and cybersecurity across all surface modes of transportation, including pipelines, thanks to the trust and relationships we have cultivated with our Federal partners and industry as evidenced by the programs and resources TSA has collaboratively developed and implementing for our surface transportation stakeholders. TSA is committed to securing the Nation's surface transportation system from terrorist activities and cyber attacks.

TSA looks forward to working with Congress on these efforts and thank you for the opportunity to discuss these issues here with you today. I look forward to the subcommittee's questions.

[The prepared statement of Ms. Proctor follows:]

PREPARED STATEMENT OF SONYA T. PROCTOR

FEBRUARY 26, 2019

Good morning Chairmen Correa and Richmond, Ranking Members Lesko and Katko, and distinguished Members of the subcommittees. Thank you for the opportunity to appear before you to discuss the Transportation Security Administration's (TSA) efforts to secure surface transportation systems including oil and natural gas pipelines from cybersecurity risks.

TSA is committed to securing the transportation sector, which includes pipelines, against evolving and emerging risks, such as cyber attacks. Partnering with our private-sector partners to secure surface transportation from cyber attacks is a critically important and complex undertaking. As the director of national intelligence recently stated, our adversaries and strategic competitors have cyber attack capabilities they could use against U.S. critical infrastructure, including U.S. surface transportation. As a disruption to any of these systems would negatively impact our econ-

omy, commerce, and well-being, the cyber attack threat is driving the Department of Homeland Security's efforts to increase the cyber resilience of surface transportation.

SURFACE TRANSPORTATION

The U.S. surface transportation system is a complex, interconnected, and largely open network comprised of mass transit systems, passenger and freight railroads, over-the-road bus operators, motor carrier operators, pipelines, and maritime facilities. The various modes that make up this system operate daily in close coordination with and proximity to one another. Americans and our economy depend on the surface transportation system operating securely and safely.

Every year more than 10 billion trips are taken on 6,800 U.S. mass transit systems, which range from small bus-only systems in rural areas to large multi-modal systems in urban areas. Over-the-road bus operators carry approximately 604 million intercity bus passengers each year. Over 3,300 commercial bus companies travel on the 4 million miles of roadway in the United States and on more than 600,000 highway bridges greater than 20 feet in length and through over 470 tunnels. Those same roads, bridges, and tunnels support the movement of goods throughout the country by 8 million large capacity commercial trucks.

As for our railroads and pipelines, more than 570 individual freight railroads carrying essential goods operate on nearly 140,000 miles of track, and 2.75 million miles of pipelines, owned and operated by approximately 3,000 private companies, transport natural gas, refined petroleum products, and other commercial products.

TSA's functions and authorities as a security agency are uniquely structured to tackle the challenges at the intersections of surface transportation and cyber risks. To secure these networks, TSA leverages its mature intelligence and analysis capability, along with its vetting and credentialing programs to ensure it can quickly develop and promulgate risk mitigation guidelines and measures to effectively coordinate and address evolving risk.

TSA's security efforts are bolstered by strong partnerships, trust, and collaboration with our Federal and industry partners. In this regard, industry works with TSA to share their own unique vulnerabilities and security needs. Through this open communication, we collaboratively develop programs and guidelines for industry to voluntarily adopt to increase their overall security posture—an approach that has yielded significant security investments and improvements beyond what the agency would have achieved from a regulatory approach alone.

We believe that this voluntary and collaborative approach to developing and implementing security measures has been successful. However, we also recognize that should the need arise, based on an imminent threat or real-world event, the TSA administrator has unique authority to require immediate implementation of certain security measures through the issuance of Security Directives (SDs).

TSA also actively collaborates with law enforcement entities, such as the Federal Bureau of Investigation (FBI), the Department of Justice, and the Joint Terrorism Task Force, to address attacks on critical infrastructure and supporting networks. For example, TSA works with the FBI to share intelligence information and host joint working groups on investigation and enforcement for attacks on surface transportation infrastructure. TSA also serves on the Energy Sector Government Coordinating Council, co-chaired by the Department of Energy and the DHS Cybersecurity and Infrastructure Security Agency (CISA), to discuss energy and pipeline security issues, provide insight on relevant intelligence, and coordinate at the Federal level on pipeline-related security recommendations and programs. Additionally, TSA works closely with the Pipeline and Hazardous Materials Safety Administration within the Department of Transportation for incident response and monitoring of pipeline systems.

TSA CYBERSECURITY ROADMAP

In December 2018, the TSA administrator issued the agency's Cybersecurity Roadmap, which will guide efforts to prioritize cybersecurity measures within TSA and across the transportation system sector over the next 5 years. The Cybersecurity Roadmap identifies 4 priorities which will help the agency achieve its cybersecurity goals:

- Identify cybersecurity risks;
- Reduce vulnerabilities to our systems and critical infrastructure across the transportation systems sector;
- Mitigate consequences if and when incidents do occur; and,
- Strengthen security and ensure the resilience of the system.

The TSA Cybersecurity Roadmap has been supplemented with the development of an implementation plan which will assist in resource allocation to this critical area. In coordination with CISA, the Federal Government's lead cybersecurity agency, the TSA Cybersecurity Roadmap brings TSA's cybersecurity efforts into alignment with both the National Cyber Strategy and the DHS Cybersecurity Strategy.

TSA'S CYBERSECURITY EFFORTS FOR SURFACE TRANSPORTATION

TSA approaches both cybersecurity and physical security by identifying, assessing, and mitigating any risks. TSA helps surface owners and operators identify vulnerabilities and risks in their operations, and works with them to develop and implement risk-mitigating solutions.

TSA's cybersecurity approach to its critical infrastructure mission is based on the National Institute of Standards and Technology (NIST) cybersecurity framework, which is designed to provide a foundation that industry can implement to sustain robust cybersecurity measures. TSA shares information and resources with industry to support adoption of the framework.

TSA cybersecurity resources and efforts for all modes of surface transportation include:

- *Cybersecurity Toolkit*.—Provides information on an array of resources, recommendations, and practices available at no cost to surface transportation entities.
- *Cybersecurity Counterterrorism Guides*.—"Pocket" resource guides to help educate all levels of surface transportation professionals on potential cyber threats, actions they can take, and best practices. Over 59,000 cybersecurity guides have been distributed across all modes of surface transportation.
- *Cybersecurity "5N5" Workshops*.—Provides owners and operators of critical infrastructure with an awareness of existing cybersecurity support programs, resources, familiarity with the NIST Framework, and an opportunity to discuss cybersecurity challenges and share best practices. Workshop participants leave with immediate benefit by receiving 5 non-technical cybersecurity actions to implement over 5 days (5N5).
- *Cybersecurity Awareness Messages (CAMs)*.—Disseminates information to stakeholders either in response to real-world events or in anticipation of significant anniversaries or holidays to support the transportation security community's efforts to increase their cybersecurity posture, and recommends voluntary cybersecurity protective measures.
- *Daily Cybersecurity Reports*.—The Public Transit and Over-the-Road Bus Information Sharing and Analysis Centers distribute daily cybersecurity awareness reports to their members.

Pipeline-specific cybersecurity efforts include:

- *TSA Pipeline Security Guidelines*.—Initially developed in 2010 and revised in 2011, the Guidelines were revised again in 2018 to align with the NIST Cybersecurity Framework. TSA added a new cybersecurity section to more accurately reflect the current threat environment to help inform industry on how best to allocate their security resources based on their operations.
- *TSA-Federal Energy Regulatory Commission (FERC) Joint Voluntary Cyber Architecture Reviews*.—Assesses the pipeline system's cybersecurity environment of operational and business critical network controls. These controls include the networked and segregated environments of Industrial Control System components, such as Supervisory Control and Data Acquisition, Distributed Control Systems, Remote Terminal Units, Human Machine Interfaces, and Process Logic Controllers.
- *Pipeline Cybersecurity Assessments*.—DHS has established an initiative to evaluate the cybersecurity posture of critical oil and natural gas pipeline systems to determine their cybersecurity practices and promote resilience. TSA has partnered with CISA to develop on-site cyber assessments of key pipeline systems as part of the Pipeline Security Initiative. The assessments will provide pipeline owners with a comprehensive evaluation and discovery process, focusing on defense strategies associated with asset owners' specific control systems network and segregated control assets. We plan to evaluate as many critical pipeline systems as possible on their cybersecurity posture by the end of this fiscal year, as time and funding allows.
- *Corporate Security Review (CSR) Program and Critical Facility Security Review (CFSR) Programs*.—CSRs are conducted to evaluate existing corporate security policies, procedures, and practices, and make recommendations for improving existing corporate security posture. The TSA CSRs have been updated to include a more comprehensive and robust review of the cybersecurity policies,

plans, and practices that the pipeline industry is employing. The CFSR program evaluates the top 100 most critical pipeline systems in the United States, collecting site-specific information from the facility operator on security policy, procedures, and physical security measures. The CFSR program assessment questions have also been updated to include cyber-specific measures.

- *Classified Briefings*.—TSA sponsors Classified briefings for pipeline owners and operators. These briefings provide owners and operators with a need to know on updated pipeline cyber threat information.

PIPELINE SECURITY SUCCESS THROUGH VOLUNTARY ACTIONS

TSA had great success in working with the pipeline community to develop and implement voluntary guidance and programs to enhance their overall security programs and raise their baseline levels of security. Specifically, the pipeline community has been very supportive and receptive to our Pipeline Security Guidelines, including the addition of a comprehensive cybersecurity section. The guidelines serve as the de facto standard for pipeline security programs, and were developed in close coordination with the pipeline industry. Major pipeline industry associations continue to show support of and collaboration with the measures set forth in the guidelines. Associations such as the American Gas Association, the Interstate Natural Gas Association of America, and the American Petroleum Institute, have written "membership statements" committing to voluntary adherence to the Pipeline Security Guidelines.

Pipeline operators have shown a willingness and ability to voluntarily implement the mitigation measures set forth in the guidelines. We have strong evidence that an industry-backed voluntary program to reduce risk by increasing compliance with the guidelines is working. TSA conducted 23 CSRs in fiscal year 2018, and those pipeline operators assessed had a 90 percent compliance rate regarding Corporate Security Program Management; an 85 percent compliance rate regarding Security Incident Management; and an 80 percent compliance rate regarding the TSA recommended cybersecurity practices detailed in the 2011 Guidelines. In addition, we have seen a strong increase in corporate compliance when comparing results from a second review to a company's first review. For 10 companies where we have conducted a second CSR, we have seen the number of recommendations made decrease from a total of 446 recommendations (first review) to 146 (second review). In addition, companies have implemented corrective actions on over 81 percent of the recommendations made during our CFSRs. This very high rate regarding corrective actions is indicative of industry acceptance and adherence to TSA Guidelines. In fiscal year 2019, we will compile similar CSR data based on the updated 2018 Guidelines, which will help determine how and where we apply additional resources to the pipeline industry.

CONCLUSION

In closing, TSA has been able to support the improvement of both physical and cybersecurity across all surface modes of transportation, including pipelines, thanks to the trust and relationships we have cultivated with our Federal partners and industry. As evidenced by the programs and resources TSA has collaboratively developed and implemented for our surface transportation stakeholders, TSA is committed to securing the Nation's surface transportation system from terrorist and cybersecurity attacks. TSA looks forward to working with Congress on these efforts. Thank you for the opportunity to discuss these important issues. I look forward to the subcommittees' questions.

Mr. CORREA. Thank you, Ms. Proctor.

I thank both of our witnesses for their comments.

Remind the Members that each one of us will have 5 minutes for questions.

I will now recognize myself for some questions. Ms. Proctor, I would like to start out with you. TSA currently relies on voluntary standards for pipeline [inaudible] tell me, is this good or bad?

Ms. PROCTOR. The approach that we use for working with the pipeline industry has been very successful. Yes, we indeed do use a voluntary approach, our Pipeline Security Guidelines were developed with the industry and they were developed to allow a voluntary involvement with the pipeline industry. What we know is

that with these guidelines we have flexibility to adjust the guidelines to the threat environment and certainly if the threat dictates, if there is a significant threat, the administrator of TSA has the authority to issue a security directive to focus on that threat and to require security measures to address that specific threat.

Mr. CORREA. So, Ms. Proctor, you are saying because of the characteristics of cyber attacks that specific regulations would be counterproductive in this area?

Ms. PROCTOR. Yes, Mr. Chairman. The nature of cyber threats is that they are constantly emerging. They are emerging—much faster than the Government's ability to write regulations to address them and in this fashion if there is a significant cyber threat the administrator may address that through a security directive.

Mr. CORREA. Any thoughts about how you would keep us as policy makers apprised of your progress or lack thereof since you are looking at really voluntary standards, self-reporting?

Ms. PROCTOR. Mr. Chairman, we would be happy to report to this committee on our progress with industry on the progress of the assessments that we conduct with industry; we actually go out and conduct corporate security reviews, looking at the headquarters, planning, the planning for cybersecurity plans, physical plans, and we go out into the field and conduct assessments at critical facilities. We conduct critical facility, security reviews in the field and we are comparing what we see in the field to the agreed-upon Pipeline Security Guidelines.

Mr. CORREA. Complying with the cybersecurity challenge can be very expensive, for the private sector or Government. So my question to you is, the private sector, do you see them complying voluntarily with what they have got to do? Which is to come up with the best practices, minimum standards or do you have to push folks to go in the right direction; do you have to push folks to do the right thing?

Ms. PROCTOR. Sir, what we have witnessed is that the voluntary approach has been very successful. We have found that the companies are making those investments in their own cybersecurity, as well physical security, and they are doing that to protect their ability to carry on their business as well so we do believe that it has been effective in this voluntary environment.

Mr. CORREA. Quickly, another area, the realignment, TSA is realigning some of its functions. Can you explain to us how this realignment will affect surface transportation security?

Ms. PROCTOR. As a result of the realignment that Administrator Pekoske has directed, the Surface Division assets are going to shift over into the security operations area where they will join with our Transportation Security Inspectors who are already in the field, that Field Force is 200-plus strong so we will be combining our surface division—our current surface division assets with the 200-plus Transportation Security Inspectors in the field, they will be working with us in conjunction with our transportation security partners in the field.

Mr. CORREA. Thank you very much.

I am going to yield the remainder of my time.

I will now recognize our Ranking Member for the Transportation Subcommittee, the gentlewoman from Arizona, Mrs. Lesko, for some questions.

Ma'am.

Mrs. LESKO. Thank you, Mr. Chairman.

My first question is for either Ms. Proctor or Mr. Kolasky, or both. Some have suggested that other Federal agencies take over the role of physical and cybersecurity for pipelines, such as the Department of Energy and I was wondering if one of you or both of you can comment on why you think that it is important that it remains under the purview of TSA and Department of Homeland Security?

Ms. PROCTOR. Thank you, Ranking Member. We do believe that the security of pipelines is best placed under the Department of Homeland Security and the assets that the Department of Homeland Security can bring to bear for the security of the pipelines.

As has been mentioned here today, we are working very closely with CISA to conduct comprehensive cybersecurity assessments on pipelines and the authority that I mentioned that the administrator, the TSA administrator has, gives him the authority to require whatever measures are necessary to secure the pipelines to be implemented almost immediately at his direction, to secure the pipelines from any type of threat, whether that threat is a cyber threat or whether it is a physical threat.

Mr. KOLASKY. If I could just add to that, Ranking Member Lesko, you know, one of the things we recognize, Sonja, and I, and our offices recognized is that we have some unique capability across DHS that we can apply to the pipeline threat and within the agency, the partnership we have established has really served as a force multiplier to TSA cybersecurity efforts.

The other thing I would augment that with, why I think this is a good place for it to be, is the fact that a lot of the nature of these risks, the control systems, the fact that pipelines contribute to other critical infrastructures are cross-sector and we really are a place and we serve as the hub to bring information across sectors when we learn about risks to some operational technologies, we can quickly get it in the hands of TSA, to get out to the pipeline owners and operators, we work together on that.

There's just a lot of shared risk in this space and separating critical infrastructure, too much across agencies you know, really runs the risk of creating stovepipes. I mean, right now we have got a nice blended mix of working with agencies, we work closely with the Department of Energy but I don't think you want to take cybersecurity responsibilities out of DHS and put them further afield because of that they are more just challenge——

Mrs. LESKO. I have one more question for, Ms. Proctor. Let me just read this from my notes. Recently the GAO determined that, in a recent audit, determined that [inaudible] risk had failed to identify critical facilities due to a lack of clarity from TSA on defining of facilities' criticality. To remedy these challenges GAO recommended that the TSA administrator take 10 actions with which TSA concurred [inaudible] what actions have been taken so that these high risks are identified?

Ms. PROCTOR. Yes ma'am. Certainly, we have reviewed the GAO report. We concur with the recommendations that GAO offered and we are in the process now of addressing those recommendations that were made by GAO. As you noted there were 10 recommendations that were made by GAO and four of those recommendations deal with the pipeline risk ranking tool that we used to help establish risk in the pipeline industry so we are diligently working on all of the recommendations but we do expect to have at least the first recommendation concluded within about 60 days.

Mrs. LESKO. Thank you, ma'am.

I yield back my time.

Mr. CORREA. Thank you, Mrs. Lesko.

I now recognize the Chairman of the Cybersecurity Subcommittee, the gentleman from Louisiana, Mr. Richmond.

Mr. RICHMOND. I will pick up where the Ranking Member left off and, Ms. Proctor, your answer indicates that you will accomplish number 1 out of 10 in 60 days, what about the other 9?

Ms. PROCTOR. Mr. Chairman, we are working on all of those 10 recommendations at the same time. We have limited resources to work on all of them at the same time so we are working to address the ones that we know that we can satisfy and those involve, again there were 4 that were associated with the risk ranking tool, so we are working directly on those, as well as the one that addresses the policy that we need to put in place for the review of the actual guidelines.

Mr. RICHMOND. Let me just give you kind of an overview of my district, largest petrochemical footprint in the country. We are neighbors to chemical facilities. We have all of the major rail lines running through our communities and for the most part they are good corporate neighbors, good employers, and they pay well.

However when we look at the risk associated with that, we have to make sure we mitigate it because on those rail cars that come through our communities are dangerous chemicals and every other thing that you can think of. So when we are looking at this, are we communicating the best, do we have strategic partnerships set up? It is important to us and so as we talk about the cyber risk for, let us say rail, and our pipelines and our oil rigs and all of those, that now a lot of that is controlled electronically.

If you think about the BP disaster which was an accident, think of a BP disaster that was an attack, so how are we communicating with those companies? But have we done anything to make sure that those companies are holding their subcontractors in their supply chain to the same high standards that we want to hold them to?

Mr. KOLASKY. So I can talk a little bit about of the nature of your question. As you know, you mentioned chemical, you know, through the CFATs regulation we put additional requirements on chemical security, some of the facilities that dealt with that. You know, you referenced the oil and natural gas industry which operates pipelines that produces a lot of what you are talking about; we work closely with the oil and natural gas industry, with the Department of Energy.

You know, specifically in terms of supply chain risk, we agree that this is an area that we have got to get deeper into, people un-

derstanding the supply chain, I think there's an understanding of that.

I referenced in my opening remarks a task force that we have established with critical infrastructure owners and operators which are focused particularly on threat information sharing, setting up processes through threat-based decision making, where should threat-based decision-making criteria be established, that will be an interagency process where we are able to get threat information out to help owners and operators make a decision about companies or products they might not want inserted in the supply chain; we are advocating, more deeply understanding what is in a supply chain, that is an important element.

But then there's also, it has to be mitigation steps, you know, are people [inaudible] again is that written in the expectation to do so in the contracts, that is the kind of stuff we are studying the Task Force to make recommendations to the Federal Government, how to do that for our own Federal networks but also for critical infrastructure owners and operators and what incentives will get people deeper in.

So you know, I would summarize a problem that we probably don't have enough information out there to help everyone be smarter buyers that could [inaudible] in talking industry we will understand why the information might not lead to the right decisions being made or us taking too much risk on, we don't want to deal with this by just cutting off things but we want a better understanding of risks that is being put into supply chains and when there are [inaudible] that could be put out there.

Mr. RICHMOND. Well, and I guess I will just say before Ms. Proctor takes a shot of it but think of passenger rail which is almost completely electronic, what are we doing to ensure the traveling public safety and do we have a sense of urgency understanding the risk that is out there?

With that, Mr. Chairman, I will yield back the balance of my time.

Mr. CORREA. Thank you, Chairman Richmond.

The Chair will now recognize other Members for questions that they may want to ask.

In accordance with our committee rules, I will recognize Members who were present at the start of the hearing, based on seniority in the committee, alternating between Majority and Minority. Those Members coming in later will be recognized in the order of their arrival.

The Chair recognizes for 5 minutes, the gentlelady Ms. Barragán, from California.

Ms. BARRAGÁN. Thank you.

I am going to actually, going to follow up on a question that Congressman Richmond just asked. In December 2016 L.A. Metro received a terror threat from abroad. It led to heightened security and this terror threat was on a commuter rail station, one that went into downtown Los Angeles, impacted about a 150,000 riders a day on this line. So my question, it was very similar to what Mr. Richmond just asked, but didn't get an answer from. So I am going to follow up there.

When we talk about cybersecurity risk, to what degree are we considering the safety of the traveling public as well, and passenger rail and mass transit rely on computerized systems; a cybersecurity attack on the system could also mean risking the safety of the traveling public. What is being done to mitigate these risks to the public and both of you can answer.

Ms. PROCTOR. We provide both information and intelligence and that intelligence is delivered sometimes in an unclassified setting but it is also delivered in a Classified setting, that is one of the most important things that we do, is keeping the systems informed about the level of threat, the type of threat, which gives them the information that they need to apply mitigating measures to that particular threat.

In conjunction with the supply chain issues that my colleague mentioned, those issues put them in the best position to ensure the safety of the traveling public. Most of our transit systems have either their own law enforcement component or they have an agreement with their local law enforcement agency to provide security for the system. We have found them to be very engaged.

We have found them to be involved not only in receiving information not only from TSA but from our colleagues at the FBI, with the Joint Terrorism Task Force and with their [inaudible] to be effective. When we receive information that suggests that some threat is present in mass transit you will often see an increased visibility; uniformed law enforcement officers including the VIPER teams from TSA, the ground-based Federal Air Marshals who support our surface transportation.

We take that information very seriously and as soon as we receive information that suggests that there might be some threat to the system and whether that threat is physical or cyber, we reach out to those systems to make sure that they are aware so they can start to apply mitigating measures.

Ms. BARRAGÁN. Right.

Mr. Kolasky, do you want to add anything to that?

Mr. KOLASKY. Yes. Let me talk to, specifically about the rail. So Sonya mentioned information sharing, we know a lot about cyber information, cyber things that might be happening but one thing we did, a couple years ago is work with the rail industry to attach cyber indicators, things that could be happening in terms of tactics, techniques of a cyber attack, to controls that would be most useful in a rail transit context. So you know, we took general information and we organized it by using the NIST Cybersecurity Framework, working with industry where we could take specific indicators and say, if you see this sort of stuff, here's what you might want to do in a rail system, it is—it is that customization that helps.

Then I would just add on the physical security which you referenced in 2016 and another thing we do DHS is you know, try to enhance soft-target security and technology development that can be deployed in transit settings you know, through our Science and Technology Directorate partnership with TSA and [inaudible] and do stuff through funding in transit systems so you know, we are getting better every [inaudible].

Ms. BARRAGÁN. Recruiting and retaining a skilled cyber work force is something the DHS and this committee has had a top pri-

ority to do. Historically CISA has struggled to fill important cybersecurity positions and I understand that TSA is also looking to grow its cybersecurity work force. Mr. Kolasky, does the new National Risk Management Center have enough of the right people to carry out the ambitious goals you described without depleting personnel from other parts of CISA?

Mr. KOLASKY. We have all pledged not to cannibalize each other so I think that is a good strategy here.

You know, we started with a good basis of analysts who have experience, thinking about strategic risk, analyzing strategic risks, doing planning, but we will be continuing hiring as we go forward to establishing the National Risk Management Center, we have about 20 positions that we are in the process of filling so you know, as a director of an organization I always want more talent; we are going to be pushing for it. I think we have the ability to recruit people, becoming the Cybersecurity, Infrastructure Security Agency is motivating us to get better candidates; we are using tools, incentives to hire people and things like that, but we want to keep pushing.

Ms. BARRAGÁN. Yield back.

Mr. CORREA. Thank you, Mrs. Barragán.

I will now call on the gentlelady from New York, Miss Rice, for 5 minutes for questions.

Miss RICE. I am familiar with one of the largest subway systems that we have in this country, New York City Subway System. It is a system that services 5.7 million people every single day, traveling through 472 subway stations and across 662 miles of track—that is 1.8 billion people per year so I wonder if there is a strategy specifically. I need to look into this with the NYPD which I think is probably one of the premier law enforcement agencies that you work hand-in-hand with.

Is there a strategy, and more importantly in New York City where everyone is very impatient, and likes to get from Point A to Point B as quickly as possible? You know, after 9/11 everything changed about how you travel, when you go into the airport.

Is there a public appetite for that kind of security system before you enter any system and I guess this is really a rhetorical question so that is just to throw that out there and I mentioned the impatience of New Yorkers because anything that slows down their travel is something that they will probably squawk about but you know, I would hate to have that be instituted after a terrible tragedy happens where the appetite might be more [inaudible] another thing, I'd like to ask you about is China's growing footprint in the United States. Industrial supply chain and infrastructure. They are rooted in part by the emergence of the state-owned China Railway Rolling Stock Corporation, CRRC for short, which I am sure you are all well aware but they have won 4 out of 5 large U.S. transportation [inaudible] has won contracts with the Metropolitan transportation authorities in Philadelphia, Boston, Chicago, and Los Angeles.

Another source I believe of the anxiety around these acquisitions concerns is the development that CRRC won these contracts by placing low bids. Many critics point to the fact that the company

receives support from Chinese government through state subsidies which other contractors do not.

But also you know, you have Members of Congress, the Pentagon, and industry experts that have stated concerns about China's capabilities in deploying Chinese manufactured subway railcars to engage in cyber espionage and surveillance, similar to the Government's concern when it comes to Huawei in the telecommunications field. What is the level of concern that either one of you have? You know, and I guess this is a supply chain question as well, but it seems to me that this is like a big red flag; I know that New York does not contract with CRRC but just your thoughts on that, it seems like just such a huge red flag.

Mr. KOLASKY. So two versions of thoughts. One thing that we have to do, what we can to protect our information to not allow China to use business information. [inaudible] There is an increased threat and risk out there.

If you ask our specific concerns about any one of these, it is less about whether it is CRRC or anything, it is about practices that have been put in place to make sure that risk isn't being introduced into the system.

So you know, this really comes into procurement questions, do we have tight procurement, let us please not go with the lowest bidder price-wise if you are a Metro Transit Authority, let us make sure that they hit pretty tough security requirements and then you can make a price-based decision but the security requirements have to be built into the contracts, part of those security requirements is looking at the manufacturing, where the manufacturer's going, getting eyes on as a procurer with technical expertise to make sure risk isn't being introduced at the point of manufacturing [inaudible] how you set up the maintenance so I don't want——

Miss RICE. Do you set up those requirements or at least the laundry list of things that States and municipalities should look at. How many States adhere to them?

Mr. KOLASKY. So, I mean, we are still in the process of working with the Transit Authorities. We had a conversation on Friday where we shared some intelligence information around that to help make decisions. Right now, I think there's an opportunity for companies to put greater requirements into procurement language, that is something that the TSA and us will be working with the industry on.

Miss RICE. So what would be the pushback against adhering to your guidelines?

Mr. KOLASKY. I think when you talk to chief operating officers, security officers, they want to do that, it is pressures that they get from other pressures in——

Miss RICE. With costs?

Mr. KOLASKY. Yes. So you know, we understand that these decisions are trade-offs. We want to be in the side of pushing hard for security, recognizing that there are other pressures, the business in the Transit Authority space.

Miss RICE. Whether it is interference in our election process which is well-documented. I mean, we have so many vulnerabilities across so many fundamental infrastructures in this country that we have to have a serious conversation about this and I just think

that if you are going to set up guidelines, we have to try to understand why States are not going to adopt them and abide by them, if you are the agency from whom they are supposed to be getting this?

Mr. KOLASKY. Sure there is good procurement in there.

We agree you know, we will set the guidelines, we will help them do that. When security-based procurement decisions or informed procurement decisions are not happening, that is where the Executive branch and Legislative branch should have a conversation about what are the limitations for that happening.

I don't know, I don't want vulnerabilities to turn into risk, they are vulnerabilities as you said but let us really take a risk-based approach to where the priority should before activity.

Miss RICE. When you come up with those guidelines, what data are you using to kind-of push that information out, what are you basing your concerns on in terms of the supply chain, the procurement process?

Mr. KOLASKY. Based on, first of all, seeing systems, so where we see vulnerabilities let us stick with elections perception, we have gone out and we have worked with States and counties to look at their election systems, see some common vulnerabilities, we do that.

Also working with the vendors in areas to understand you know, areas where additional guidelines would help their own security side and taking advice through these protected conversations, through the Critical Infrastructure Partnership Advisory Council structure, we are hearing me, as somebody who wants to make a security decision, do not feel like I have all the information I need to make a security decision. So it is these conversations that help us.

Miss RICE. Do you have anything that you want to add?

OK.

Thank you. I yield back.

Mr. CORREA. Thank you, Miss Rice.

I will call in the gentleman from Rhode Island, Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

I want to welcome our witnesses here today and thank you for your testimony.

Before I begin, I just want to mention I concur with Chairman Thompson [inaudible] keep the pipeline, cybersecurity in the realm of TSA and not see it shipped over to DOE so I think that is an important point to make and I am glad that it is been raised here today.

Obviously with all this and I think this hearing is essential to focus on transportation security especially to cybersecurity, these are the things that keep me up late at night you know, as you know, where is the most damage that can be done is in the area of critical infrastructure, in a number of fields and so one of the aspects I want to focus on today is on pipeline security and obviously you need the right policies and procedures and plans put in place, you need the right people with the right expertise.

So, Ms. Proctor, let me start with you, December 2018 GAO report indicated that staffing in the Pipeline Security Division was a major challenge with a number of empties ranging from 14 all

the way down to 1, across several fiscal years. What is the current staffing level of the Pipeline Security Division?

Ms. PROCTOR. Today the current staffing level is 5 but I think it is important to say that with the realignment that has been directed by the administrator, we will be shifting into the Security Operations organization where we will have the benefit of the additional Transportation Security Inspectors in the field. You know, there are 200-plus of them that will serve all of surface transportation so our Pipeline Section will be much larger, we will draw from that pool of Transportation Security Inspectors to provide the training and the experience to put them in the Pipeline Section.

Mr. LANGEVIN. How many do you estimate will be in and specifically dedicated to pipeline security, or are you talking about, they are going to be leveraged across all those fields and from time to time they will rotate into the pipeline security, I am not clear on your answer?

Ms. PROCTOR. Well, we think the Pipeline Section is going to require specialized training so we are going to put those people in there, provide the training and make sure that they are qualified to go out and do those assessments.

We have not arrived at a final number yet, we are still working on some of the staffing issues or the shifting of personnel because it will serve all of our surface transportation partners in a way that is going to allow us to put more people in the field working directly with our surface transportation partners.

Mr. LANGEVIN. So of the 5 that you mentioned, those staff, how many have expertise in cybersecurity specific?

Ms. PROCTOR. I am sorry we have none that have specific cybersecurity expertise. They do have pipeline expertise but not cyber expertise.

Mr. LANGEVIN. I find that a troubling answer but let me ask you, across all TSA services, service transportation of course, how many specialize in cybersecurity?

Ms. PROCTOR. TSA does not have cybersecurity specialists. We rely on our colleagues at CISA for cyber expertise. I mean, that is a specialized field so we do rely on the DHS experts to provide that input and they have, we work directly with them when we were developing the Pipeline Security Guidelines, and got input from them to develop the current Pipeline Security Guidelines that have a cybersecurity section in them.

Mr. LANGEVIN. OK. So we will stay on the topic of pipeline security, approximately how many Critical Pipeline Systems are there again in the United States? You maybe talked about this earlier on, but——

Ms. PROCTOR. That number varies depending on mergers and acquisitions, the number we work with is somewhere around a 120.

Mr. LANGEVIN. OK so I [inaudible] at end of the year, I mean, in your view given the number of pipelines that we are talking about, is that adequate? Because it does not seem so to me.

Ms. PROCTOR. I don't want to suggest that those are all of the pipeline assessments that we do so we still do critical facilities, security reviews and those are separate from the 10 comprehensive cyber assessments that we are doing with CISA so we will continue to do those critical facilities security reviews. We completed 62 of

those last year, even given the resources that we are working with now, but the 10 that we are referring to are going to participate in the Comprehensive Cyber Security Assessments that we are doing with CISA.

Mr. LANGEVIN. OK, before my time runs out, I want to ask you, Ms. Proctor, again the TSA Cybersecurity Roadmap provides for the development of an implementation plan to see it put into practice so had the actual implementation plan then developed?

Ms. PROCTOR. We are in the process of developing that plan now. You know, we recognize the priorities in the cybersecurity plan and the value that it is going to bring to us in surface transportation. That plan is relatively new but we are reviewing that plan now to determine how we can implement that in surface transportation.

Mr. LANGEVIN. When do you think the plan will actually be finalized and is Congress going to be provided a copy of that? Because we would like a copy.

Ms. PROCTOR. We would be happy to provide a copy of that finalized plan and I can certainly provide you an update on when—when we believe that is going to be finalized. As indicated, we are working through a number of requirements right now including the GAO requirements so we are working on all of those concurrently.

Mr. LANGEVIN. All right. Before my time runs out, I just want to ask this though, how do you expect the [inaudible] with the rollout of the Roadmap and what additional resources, if any, are required to carry out the new plan once it is finalized?

Ms. PROCTOR. The Cybersecurity Roadmap is going to require more coordination with CISA and we will have to determine the resources based on how we see that plan rolling out and how we see it being implemented across all of the surface transportation modes, but we have been working very closely together, so those are some things that we are going to have to continue to work and to ensure that we can carry out the administrator's intent on that plan.

Mr. LANGEVIN. But the resources are going to be factored in, and actually as the plan is finalized you are working through those additional resource requests now as well?

Ms. PROCTOR. I am sorry, I didn't——

Mr. LANGEVIN. You are planning for additional resource requests once the plan is finalized, is what I am hearing you saying, correct?

Ms. PROCTOR. Yes sir.

Mr. LANGEVIN. OK.

Thank you very much.

I will yield back.

Mr. CORREA. Thank you, Mr. Langevin.

Now would like to call the gentlewoman from New Jersey, Mrs. Watson Coleman, for 5 minutes of discussion.

Mrs. WATSON COLEMAN. Thank you, Mr. Chairman.

Thank you very much for your testimony. What is the greatest threat from a cybersecurity attack on the pipeline? Is it that it would cut the flow of the natural gas or is it that it would blow up, what is it?

Ms. PROCTOR. So we recognize that the threats to pipeline from a cyber perspective do exist. Most of our significant pipelines are

controlled to some extent by computer systems that manipulate valves and switches and controls——

Mrs. WATSON COLEMAN. Right.

Ms. PROCTOR. So that impact would more likely affect the operation of the system. We would assume that it would affect more the operation of the system, the flow perhaps of the commodity.

Mrs. WATSON COLEMAN. Is there any other kind of threat that could result in either a leakage or an explosion that could be triggered by some nefarious actors?

Mr. KOLASKY. So I think we would like to have a follow-up conversation with you about threats where we can be more specific in a different setting. I don't mean to put you off——

Mrs. WATSON COLEMAN. OK.

Mr. KOLASKY. But I think that is more appropriate.

Mrs. WATSON COLEMAN. Thank you, because I am concerned. Do you work with FERC at all?

Ms. PROCTOR. Yes ma'am, we do.

Mrs. WATSON COLEMAN. Because in New Jersey, in my district, there's a PennEast pipeline and I visited a home and the pipeline is going through that person's yard and as close as you are to me, is as close to the pipeline is to the woman's bedroom and so things like that concern me about the siting of these pipelines but in addition FERC hasn't had the responsibility, the requirement of saying whether the pipelines are in the vicinity and that could be somehow accessed so that we don't have so many pipelines, we just have the efficiency that we need and you don't deal with that issue with FERC at all in terms of siting, right?

Ms. PROCTOR. No ma'am. We don't deal with the issue of siting at all. We do work closely with FERC and we have conducted Cyber Architecture Assessments with FERC so——

Mrs. WATSON COLEMAN. But that is not proximity. That is not location, that is infrastructure, right?

Ms. PROCTOR. Correct.

Mrs. WATSON COLEMAN. If we have to have this conversation in another setting but we keep talking about the vulnerabilities that exists either in supply chain or in cybersecurity or in any way impacting the safety and security of any rail transportation, any pipelines and we say that we are doing things to advise our clients, whomever of these vulnerabilities.

Can you tell me in this setting: (A) How we identify these vulnerabilities, and (B) how does the procurer ensure that there's language or whatever that protects that item that they are purchasing that is being built by China or anybody else? Is that something that we can discuss here?

Mr. KOLASKY. Yes. To some extent. I mean, first of all, I want to reinforce that most of these worst-case scenarios, there is a lot of fail-safes, there's layered defenses broken, built in here and you know, one of our overall strategies is to get better, better, better to make this stuff, the worst case that you are imagining, incredibly complex and only accomplishable by having physical access or doing things that are likely to be picked up by a Layered Defense System.

So first and foremost strategy, it is better understanding what is already put in place and putting in places to share information as

quickly as possible. When you make something really complex just like with a terrorist attack, you are more likely to see the plotting that is going on there——

Mrs. WATSON COLEMAN. Yes.

Mr. KOLASKY. We have come a long way in that direction. Our adversaries might continue to get better but you know——

Mrs. WATSON COLEMAN. Yes.

Mr. KOLASKY. By making things complex is a good risk management strategy.

Mrs. WATSON COLEMAN. But I also want to know that when you are purchasing rail cars, what is it that you tell the agency that is advertising, these specific things are how you mitigate the possible compromising of the safety and security of your car or whatever?

Mr. KOLASKY. Sure. So——

Mrs. WATSON COLEMAN. And——

Mr. KOLASKY. At the basic level we give them an overview of business practices of companies and links to Chinese intelligence doctrine, things that are available to understand that there may be——

Mrs. WATSON COLEMAN. I am going to assume——

Mr. KOLASKY. Risks introduce into the system and then we talk through what good procurement strategies are.

Mrs. WATSON COLEMAN. I want to assume, worst-case scenario, that we are purchasing cars from a company that means us no good. I want to know specifically how do we protect against that—what do we look for specifically to make sure that whatever thing is that might compromise the safety of that car and its passengers. How do we see it, how do we know it, how do we look for it? [inaudible]

Mr. KOLASKY. It leads to a follow-on discussion.

The last thing I would say is that one of the things we are bringing in from a procurement perspective is the Federal Government as a whole has experience in procuring things that are really, really important to us and need to be secure and so part of what we can do with DHS working with some of our folks who do even bigger procurement is bring some of those practices, share that with industry around so the relationship with us and DOD and that sort of—in the testing that goes on in National Labs, that stuff's really important to get to——

Mrs. WATSON COLEMAN. OK.

Mr. KOLASKY. The level of fidelity you want.

Mrs. WATSON COLEMAN. So I thank you.

My time is up and I just want to say, Mr. Chairman, I somehow would like to have a discussion in another environment as to exactly what these things are.

Mr. CORREA. I would love to do that, if we can I will.

Mrs. WATSON COLEMAN. Thank you very much.

Mr. CORREA. I will talk to the staff and, Mrs. Watson Coleman, let us see if we can do that.

Thank you very much and recognize Ms. Slotkin for 5 minutes of questions. Thank you.

Ms. SLOTKIN. Yes. Hi, sorry to be late. I apologize. I am happy to be the only one at this giant table down here.

I apologize if this is slightly repetitive. I like the—some of my other fellow Congress men and women, have pipelines going through my district, some of them extremely close to the homes, many of them the route had been changed without the citizens' awareness and there's a lot of citizens who are concerned about their safety, as we all would be.

So can you just walk me through in sort-of clear terms No. 1, what you have done to prevent cyber attack and then No. 2, if there's a specific threat or a risk; I am from the intelligence community, former CIA officer and was definitely aware that there was plenty of time, there were Classified information, threats, concerns, new techniques, that were Classified so we couldn't actually communicate with local businesses, with local communities, local law enforcement, even on the real nature of the threat so what have—what are we sort-of doing to protect ourselves and then tell me about your modus operandi on presenting information down to unclassified users?

Ms. PROCTOR. So with regard to the threat and this goes back to our information sharing. Two weeks ago, I believe we had a Classified briefing with members of the industry. It was a Top-Secret Classified briefing to talk about the threat. As a matter of fact, tomorrow we have another meeting with another Classified briefing with industry so we have found ways with our intelligence colleagues of providing the necessary information that our industry partners need in order to protect their industry from cyber threats so from the intelligence perspective we have been able to manage that with our intelligence partners.

I don't believe that there has been an unresolved issue with the intelligence that we are providing. We are providing everything that we can provide in the appropriate atmosphere, with people who have the appropriate clearances so in terms of the information I believe that we are getting that out to the right people.

Mr. KOLASKY. And——

Ms. PROCTOR. On the—cyber side, I am going to let——

Mr. KOLASKY. You referenced community-level law enforcement, and this is where the fusion centers, the DHS, sponsors, come in very handy, there are somewhere around 85 around the country and both with industry but more particularly with law enforcement and people who have been close to community-level decisions [inaudible] teleconferences and things like that.

Then implied in your question, obviously is not everyone is going to have a clearance no matter how good we get at doing that so you know, we want to push, giving more out, the unclassified assessment, as you probably can guess what was in the Worldwide Threat Assessment that Director Coats talked about, that takes a while to get that statement to be made but that statement becomes important because it lights a fire on the importance of this issue and we have been following up with industry both in the Classified and unclassified community space with that.

Ms. SLOTKIN. So related to that, if there was an incident and because of declassification or problems with sharing, that information did not get to the company, who is the senior accountable official, who would be responsible for that mishap, would it happen?

Mr. KOLASKY. We within CISA have the ability to give private-sector clearances out so we will facilitate private-sector members getting access to information, depending on the nature of the information you are talking about it is on us as a Government, who have that information to give as quickly as possible to the cleared community. I am not going to speculate on the exact hypothetical—it is our job to make sure we have opened up the channels to give Classified information.

We in other parts of the Government also have 1-day reading authorities where if you don't have a clearance but you need to have this information and so you know, I think we all feel obligated to make sure that information gets in the hands of somebody who could do something as soon as possible once we know that is credible information.

Ms. SLOTKIN. OK. I would just say, again CIA and FBI weren't communicating particularly well during 9/11. There has to be accountability if there's mistakes; I am not saying anyone's you know, God forbid, planning for mistake but it is nice to know that you know, who is responsible for making sure we pushed down this information to industry.

But I will yield back the rest of my time.

Mr. CORREA. Thank our witnesses for your comments.

Now if I may, I would like to take a 5-minute recess and then come back and start with our second panel.

Members please try to be back in 5 minutes. Thank you very much.

[Recess.]

Mr. CORREA. The committee will now come to order.

We will start with our second panel.

Our first witness is Mr. James Lewis, serves as senior vice president and the director of the Technology and Public Policy Program at the Center of Strategic International Studies.

Next we will have Ms. Rebecca Gagliostro, my apologies, who is the director of security, reliability, and resilience at the Interstate Natural Gas Association of America which is comprised of 27 members representing a vast majority of interstate natural gas transmission pipeline companies.

Next, we will have Mr. Erik Olson, who is a vice president of the Rail Security Alliance, which is a coalition of North American freight, rail car manufacturers, suppliers, unions, and steel interest.

Finally, will have Mr. John Hultquist, who serves as director of intelligence and analysis at FireEye. He has over 10 years of experience, covering cyber espionage, hacktivism, and has worked in senior intelligence analyst positions in the Department of State.

Without objection the witnesses' full statements will be inserted to the record.

I will ask now each witness to summarize their statements for 5 minutes, beginning with Mr. Lewis.

Thank you, welcome sir.

STATEMENT OF JAMES A. LEWIS, SENIOR VICE PRESIDENT, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

Mr. LEWIS. Thank you. I thank the committee for the opportunity to testify.

We have entered an era of connected devices sometimes called the internet of things that offers real economic benefit but comes with increased risk to homeland security and much of this risk comes from the global supply chain. Most infrastructure and transportation systems as you have heard are connected to the internet in some way and depend on computers for their operation. This includes electrical power systems, pipelines, telecommunications and increasingly vehicles which continuously connect back to their manufacturer wherever that manufacturer is located and these connections provide opportunities for espionage and service disruption.

As the committees have heard for many years, the state of cybersecurity remains poor. Most networks can be hacked, cyber crime continues to grow, and cyber attack is an essential part of state conflict.

Our task is to mitigate risk. One way to do this is to ask how a device connects to the internet, what information it transmits, and how much transparency and control an operator has over this data and connection.

Another way is to use three metrics: The value of data collected; the critical [inaudible] variable data; perform critical functions or whose disruptions could produce mass effect, need to be held to higher standards.

Currently the internet of things is probably more vulnerable to disruption than the regular good old internet. For critical infrastructure we can ask how we would continue to operate in the event of a malicious incident and to what degree our control over these infrastructures are shared with a foreign manufacturer.

Products from China require special attention. The combination of increased Chinese espionage, new national intelligence law on China, pervasive surveillance, and heightened military tensions have led to a dangerous situation but the United States and China share a deeply integrated industrial base, disentangling this would be costly, although some now talk of a divorce. China is not the only country that could exploit cyber vulnerabilities and critical infrastructure. Iran and Russia have probed pipelines and other infrastructures, including electrical power.

There are several steps we can take to reduce risk. The most obvious is to improve network and device security. DHS's Cyber and Infrastructure Security Agency, CISA, should be the center of this effort.

The development of security standards is essential. The NIST Cybersecurity Framework is a strong start but it needs to be amplified and expanded for specific technologies. Any defensive measure must accept that we cannot keep a determined opponent out of our networks. This means that we must also consider measures to increase resiliency and allow for continued operation, integrated environments; this is the goal that DOD has. Better security requires oversight. This is clearly a task for the committee but also for CISA.

Finally, a defensive approach by itself is inadequate. The United States needs to develop credible threats to deter foreign attackers and persuade them that interference in critical infrastructure comes with the unacceptable risk of retaliation. We do not have this now. That would be a useful thing to do.

We haven't talked about the security premium which is what many of us call it, it has come up several times [inaudible] in part because it is subsidized by the government. There might be a Chinese intent, it is worth looking at, this subsidy but it means for companies—and we see this particularly with Huawei—they must choose between buying cheap good equipment or more expensive equipment that is secure, and that is a difficult choice. I am not sure everyone will always come out in the same place.

Thank you for the opportunity to testify. I look forward to your questions.

[The prepared statement of Mr. Lewis follows:]

PREPARED STATEMENT OF JAMES A. LEWIS

FEBRUARY 26, 2019

I would like to thank the committee for the opportunity to testify. My testimony will discuss the risks to homeland security from the use of Chinese technology and equipment.

Chinese companies face a serious branding problem in many countries. There is a level of distrust that has been created in good measure by Chinese government policies. The most prominent of these policies are China's aggressive mercantilism, its disregard for international law, its massive espionage campaign, and, for the United States, its announced intention to displace America and become the most powerful country in the world, reshaping international rules and practices to better fit the interest of China's rulers.

Espionage has been a part of the of the Sino-American relationship since China's opening to the West in 1979. It is worth remembering that at this time, the United States and China shared a common enemy—the Soviet Union. This created incentives for cooperation that have long vanished. Chinese espionage initially focused on repairing the disastrous effects of Maoist policies on China's economic and political development. This meant the illicit or coercive acquisition of Western technology. As China's cyber capabilities improved, beginning in the late 1990's, some PLA units turned to hacking as a way to supplement their incomes, moonlighting by stealing Western intellectual property and then selling it to Chinese companies.

The illicit acquisition of technology is still a hallmark of Chinese espionage activity, but there have been significant changes since President Xi Jinping came to power in 2013. One of the first things Xi did, reportedly, is order an inventory of Chinese cyber espionage activities. He found that many of these had not been ordered by Beijing, that Beijing did not have full control over tasking and assets, and some operations were for private interest and did not meet China's strategic requirements.

Xi changed this. The Chinese military has been reorganized as part of a larger effort to modernize the PLA. Xi's anti-corruption campaign greatly reduced the ability of PLA units to "moonlight." Chinese intelligence collection is better organized, more focused on strategic priorities, and, some would say, better in performing its missions. This comes at a time when, according to the U.S. intelligence community, Chinese espionage has reached unprecedent levels. Today, these efforts focus on the acquisition of advanced military and commercial technologies, since China still lags the United States in technology, as well as military and government targets.

The United States and China reached an agreement in 2015 to end commercial cyber espionage, but it is generally believed that this agreement has broken down in the last year. At the risk of sounding overly dramatic, some would describe this situation as an undeclared espionage war between China and the United States. In fact, this is not a war, but a very intense contest where the United States is largely on the defensive. Our allies also face a similar problem with Chinese efforts in Australia, Japan, Germany, the United Kingdom, Canada, and other advanced economies.

These activities create distrust, and a more specific ground for distrust is China's 2017 National Intelligence Law. For some years, the United States had advised China to move away from an informal, ad hoc system of rules and put in place a formal legal structure based on laws. The Chinese took our advice and one result is that long-standing Chinese policies and practices have been codified into the 2017 Intelligence Law. The most important part of that law for today's hearing is that it creates a legal obligation for Chinese companies to cooperate fully with intelligence agencies upon request. There are no grounds for appeal or an ability to refuse such requests.

This means that a Chinese company could be completely innocent of any wrongdoing, its products harmless, but a decision by the Chinese government could change that in an instant. In the context of an increasingly aggressive global espionage campaign, often conducted using cyber techniques, there are reasonable grounds for the distrust of Chinese products. The first question to ask is not whether you trust a Chinese company, but whether you trust the Chinese government.

Concerns over the Intelligence Law have become so significant, in part because of the implications of using Huawei telecommunications equipment, that China's official news agency felt obliged last week to put out a press release calling for a comprehensive and accurate translation. China's Foreign Ministry pointed out that while Article 7 of the law stipulates the obligation for Chinese companies and individuals to "support, assist, and cooperate" with the country's intelligence service, Article 8 stipulates that China's intelligence service should carry out its work according to law, protect human rights, and safeguard the legal rights and interests of individuals and organizations. Unfortunately, this promise is undercut by China's recent behavior in regard to human rights and in the protection (better expressed as the absence of protections) for the intellectual property of foreign companies.

We should note that China's government expresses similar concerns over their reliance on Western technology, in part because they assume the relationship between Western companies and government is the same as the relationship between Chinese companies and the government. This official distrust of Western products is one reason why Beijing is spending billions of dollars to develop national sources of supply for many technologies. These subsidies also provide commercial benefit, in building national champions in Chinese industry and in eroding Western companies' market position.

China also leads the world in building a national system of pervasive domestic surveillance. Communications and social media are monitored, and an array of sensors monitor and record activities in urban areas. This sensor data is correlated with information held by the government on Chinese residents' behavior and communications. This pervasive surveillance is not popular among many Chinese, but it is increasingly difficult to escape. One concern is that China will to some degree extend this pervasive surveillance to countries and persons of interest outside of China or extend its extensive cyber espionage campaign to include coercive actions, like disrupting critical services. This is not something China would do lightly, but the risk cannot be dismissed.

The combination of increased espionage, new legal obligations, pervasive surveillance, and heightened military tensions make for an uncomfortable and potentially dangerous situation, with implications for U.S. security. The United States and China share a deeply integrated industrial base, constructed during the time when we assumed that China was moving in the direction of becoming a market economy and a security partner. Disentangling this deeply integrated supply chain would be costly and damaging to both countries, but some in America now talk about a "divorce" while China is spending heavily to reduce its reliance on the United States.

Beyond the espionage risk, there is potential risk for critical infrastructure that is growing. As more devices become connected to the internet and reliant on software, the opportunities for disruption will grow. This is not specifically a China problem, but a change in the technological environment as millions of devices connect to the internet in ways that China (or other malicious actors) could exploit for coercive purposes.

As the committee has heard for many years, the state of cybersecurity remains poor and almost any network or device can be hacked with enough persistence. Cyber crime continues to grow, and cyber tools have become an essential part of state conflict. If it is any consolation, China's cybersecurity is worse than ours, if only because of their frequent use of pirated software. Improving cybersecurity should be a potential area for cooperation between the two countries, but the current state of relations does not permit that.

An environment of connected devices, often called the internet of things, is formed by devices that connect to the global internet, usually without human intervention. We all have heard of smart cars but many large systems in infrastructure and

transportation also rely on computers and connectivity. This environment will provide real economic opportunities and benefits, but it also comes with an increase in risk. Our task should be to estimate this risk and then develop strategies to mitigate it. Different technologies and different companies create different levels of risk, and there are several ways to assess this.

One way to scope risk is to ask how a device connects to the internet, what onboard sensors it has, what information it collects and transmits, and how much transparency, insight, and control an operator has over this data and connection. Many large capital goods, such as power technologies, pipelines, telecommunications and ships, are continuously connected over the internet to their manufacturer, to allow for status reports, maintenance scheduling, and for the updating of software. This continuous connection provides an opportunity to collect information and to disrupt services. Instead of an update, a command could be sent to turn off or to reduce speed.

We have seen several examples of Chinese devices that report home, from drones to surveillance cameras, with the concern that under the new intelligence law, the Chinese government could compel the provision of the data collected by these technologies. This kind of monitoring and collection has been a standard practice for intelligence agencies that will certainly extend to the internet of things, and the risks of connected devices is compounded when their home is in a hostile foreign power.

We could scope risk by measuring the cybersecurity status of connected devices. The National Institute of Standards and Technology (NIST) is developing, in partnership with industry, standards for the security of IOT devices. But this is still at a relatively early stage. In general, the internet of things will be no more secure than the existing internet and may be more vulnerable, since many IOT devices will use simple computers with limited functionality.

We can also assess risk by using three metrics—the value of the data accessible through or collected by the IOT device, the criticality of a function the connected device provides, and scalability of failure. Devices that create or collect valuable data, perform crucial functions, or that can produce mass effect, need to be held to higher standards and face greater scrutiny.

For critical infrastructure, we need to ask the same questions about using Chinese products that we would ask for any critical infrastructure protection policy: How sensitive are the operations and the data associated with or accessible through the infrastructure, what would happen if the infrastructure was disrupted by an opponent, how would we continue to operate and then recover in the event of a malicious incident, and for foreign products, and to what degree is control or access shared with the foreign manufacturer?

The type of data collected and transmitted is a crucial element of a risk assessment. Intelligence analysis data is driven by access to large amounts of data and the ability to correlate it with other data. Data analytics provides new intelligence insights. A well-known example is the hack attributed to China of the Office of Personnel Management (OPM) and the theft of personal information. It is likely that OPM was one of a series of related hacks, of insurance companies, airlines, and travel agencies, that provided additional data that could be used to gain insight into America, personnel and practices. This means that even seemingly insignificant data, if correlated with other information, may provide influence value. The more "granular" the data, and whether it refers to specific individuals, the greater its value. Less granular data, such as how many people are sitting on a train or at which stop they exit, may not pose much risk.

Managing our new competition with China will be difficult given the close interconnection between the U.S. and Chinese economies. This is a 30-year commercial and technological partnership not easily dismantled by either side. Given the deep interconnections that have grown between the Chinese economy and the rest of the world, a bifurcation similar to that seen during the Cold War is not possible, and it is not now in our interest. A greater degree of separation between the two economies is necessary but must be carefully developed for specific technologies and based on a judgment on the risk that their use could provide China with an intelligence, military, or unfair commercial advantage.

These risks are manageable, and we have to contrast them to the risk to the America economy from a violent disruption of trade with China. Generally speaking, a complete divorce is not in our interest; and it is certainly not in China's interest. There are specific technologies and circumstances that require greater scrutiny and countermeasures, but this does not apply across the board (at least at this time). Working with our allies, we can modify China's behavior to make this relationship more stable and less risky. We have done so in the past, but this will be a process that will take years to complete, and in the interim, there are steps we must take to reduce the risk of Chinese interference and espionage.

The most obvious is continued work to improve network and device security. This will require some measure of regulatory action and close partnership with the affected industries and operators. One size does not fit all when it comes to regulation, so the potential risk of IOT and Chinese technology must be managed using the sector-specific model developed in the previous administration, and partnerships between companies, agencies with oversight, and DHS's new Cybersecurity and Infrastructure Security Agency (CISA) should be the core of this effort.

The development of security standards is a necessary complement to any regulation or voluntary action. The NIST Cybersecurity Framework is a good starting point for this but must be extended and modified for different kinds of transportation systems. CISA's Transportation Systems Sector Cybersecurity Framework Implementation Guide, published in June 2015, provides guidance to owners and operators on how to assess and implement cybersecurity standards.

All of these measures—voluntary action, regulation, and standards—must be predicated on the knowledge that we cannot keep opponents out of our networks and devices. We can make it harder for them but not impossible. This means that measures to increase resiliency, to allow for some level of continued operation in degraded conditions is essential. This adds expense to critical infrastructure, of course, and one part of any plan is to ask how this additional burden will be funded and whether the increase in risk is outweighed by the potential savings—we should not automatically assume that the mere existence of risk cancels out financial benefits.

All of these steps require oversight to assess risk and improvement. This is clearly a task for Congress and this committee, but also for the responsible agencies, industry bodies, and, in particular, for CISA. The key question for assessment is whether the use of the Chinese technology increases the risk of disruption or espionage, and the answer to this will depend in good measure on how the Chinese products connect to the internet.

Finally, a purely defensive approach will be inadequate. The United States needs to develop and articulate credible counterthreats to dissuade and deter foreign attackers. This may require more than sanctions and indictments. Although they are useful and have effect over the long term, they may need to be reinforced other punitive measures, part of a larger strategy on how to impose consequences and change opponent thinking. Given the level of vulnerability and the potential increase in risk from both the acquisition of foreign technology and the digitizing of critical services, we must persuade opponents that any interference will come with unacceptable risk or retaliation by the United States.

There are trade issues that I have not touched upon, such as the Chinese practice of building national champions through government subsidies and, in some cases, industrial espionage. China also uses non-tariff barriers and other protectionist mechanisms to hobble or block competition from foreign firms in China. These Chinese practices harm our National interests and should be opposed as part of a larger effort to change China's behavior and move it in the direction of reciprocity.

I thank the committee for the opportunity to testify and look forward to any questions.

Mr. CORREA. Thank you, Mr. Lewis.

Now I would like to recognize, Ms. Gagliostro, to summarize her statements in 5 minutes.

STATEMENT OF REBECCA GAGLIOSTRO, DIRECTOR, SECURITY, RELIABILITY, AND RESILIENCE, INTERSTATE NATURAL GAS ASSOCIATION OF AMERICA

Ms. GAGLIOSTRO. Thank you.

I am delighted to be here today to share our thoughts on cybersecurity in the pipeline industry. My name is Rebecca Gagliostro, director of security, reliability, and resilience at the Interstate Natural Gas Association of America.

INGAA is a trade association that advocates regulatory and legislative positions of importance to the Interstate Natural Gas Pipeline Industry. Our 28-member companies operate approximately 200,000 miles of interstate natural gas pipelines that are analogous to the interstate highway system. Like the highways that are the arteries for so much of our Nation's commerce, interstate natural

gas pipelines are the indispensable link between U.S. natural gas producers and consumers.

In my role at INGAA, I work directly with our members to ensure that our pipeline infrastructure remains resilient, safe, and secure. Cybersecurity is a priority for the Natural Gas Pipeline Industry. INGAA member companies work worked diligently to secure our Nation's critical gas transmission infrastructure from both cyber and physical security threats. Cybersecurity has been identified as the top operational risk by the executive leadership of our member companies and we take the management of this risk very seriously.

Last year in recognition of this priority, INGAA's board of directors set forward with its commitment the Pipeline Security Statement. This Statement enumerates specific actions that all of our member companies are taking as part of their security program. The Statement emphasizes among other things, our commitments to following the Transportation Security Administration's Pipeline Security Guidelines.

Industry security efforts seeks to reduce the risk posed by successful attack targeting our infrastructure. A foundational element of a well-informed risk management program is comprehensive information sharing. This is the key point that I would like to emphasize. Real-time actionable information is vital to ensuring our pipeline operators are equipped with the latest intelligence on threats.

Information sharing is occurring today between INGAA member companies and other industry stakeholders through the work of our Information Sharing and Analysis Centers also known as ISACs, however this is not industry's responsibility alone. It is imperative that we also have a cooperative working relationship with our Government partners to help facilitate information sharing.

We would like to note that there is strong information sharing occurring today with our partners at TSA and the Department of Homeland Security and we would like to see this relationship continue.

INGAA believes that TSA's Pipeline Security Program is making a difference as it continues to improve. We understand that TSA has accepted the Government Accountability Office's recommendations for improving the management of its Pipeline Security Program and it is now in the process of implementing changes in response to those recommendations. INGAA strongly believes that if followed these recommendations will help to make a stronger and more robust program.

The increasing threat of nation-states cybersecurity attacks and interdependencies across our critical infrastructures means that we must work together across industry and Government to protect ourselves against threats. The work that TSA and the Department of Homeland Security are doing with the National Risk Management Center is a very positive step toward the end goal of protecting the Nation from cybersecurity threats.

Threats to critical infrastructure cannot be evaluated in isolation; all critical infrastructures are being targeted, therefore we must identify the best ways to work together to protect our National security.

In October, TSA and DHS announced their joint partnership in the Pipeline Cybersecurity Assessment Initiative which is working to conduct Comprehensive Cybersecurity Assessments to pipeline infrastructure. Assessments play a critical role in providing the assurance that these programs are working. TSA has already piloted one INGAA member assessment in 2018 and our members continue [inaudible] we believe that progress has been made in securing our pipeline infrastructure and we should continue to focus on improving TSA's Pipeline Security Program.

The growing threat of nation-state cyber attacks requires a coordinated and comprehensive approach backed by strong information sharing across all critical infrastructures sectors and across all Federal agencies supporting National Security. TSA's on-going work with the National Risk Management Center is helping to bridge that gap.

We urge Congress to support TSA's efforts to improve its program and provide the necessary guidance and funding for additional program-management staffing and cybersecurity expertise that can work alongside the National Risk Management Center and support the Pipeline Cybersecurity Assessment Initiative. We believe that this, in addition to the efforts that are already under way, will help to make TSA successful in its mission to protect the Nation's pipeline infrastructure. Thank you.

[The prepared statement of Ms. Gagliostro follows:]

PREPARED STATEMENT OF REBECCA GAGLIOSTRO

FEBRUARY 26, 2019

Good morning Chairmen Correa and Richmond, Ranking Members Lesko and Katko, and Members of the subcommittees. I am delighted to be here today to share our thoughts on cybersecurity in the pipeline industry. I am Rebecca Gagliostro, the director of security, reliability, and resilience at the Interstate Natural Gas Association of America (INGAA). INGAA is a trade association that advocates regulatory and legislative positions of importance to the interstate natural gas pipeline industry in the United States. INGAA's 28 members operate approximately 200,000 miles of interstate natural gas pipelines that are analogous to the interstate highway system. Like the highways that are the arteries for so much of our Nation's commerce, interstate natural gas pipelines are the indispensable link between U.S. natural gas producers and consumers. In my role at INGAA, I work directly with our members to ensure that our pipeline infrastructure remains resilient, safe, and secure.

Cybersecurity is a priority for the natural gas pipeline industry

INGAA member companies work diligently to secure our Nation's critical gas transmission infrastructure from cyber and physical security threats. The boards of directors and executive leadership of our member companies have identified cybersecurity as a top operational risk and take the management of this risk very seriously. Last year, in recognition of this priority, INGAA's board of directors stepped forward with its *Commitments to Pipeline Security*[1] statement, which enumerates specific actions that all of our member companies are taking to identify, protect, detect, respond to, and recover from security threats targeting our systems. In addition, the statement emphasizes our members' commitments to following the *Transportation Security Administration's (TSA's) Pipeline Security Guidelines* and the *National Institute of Standards and Technology's (NIST's) Cybersecurity Framework,* and to engaging in comprehensive information sharing across the industry and with our Federal partners. These are the foundations to building and maintaining strong pipeline security programs.

INGAA's commitments provide a high-level roadmap of what our member companies are doing to secure our infrastructure, as appropriate for public dissemination.

[1] *INGAA Commitments to Pipeline Security, https://www.ingaa.org/File.aspx?id=34310&v=db10d1d2.*

In practice, our members' security programs are far more extensive than the information that may be conveyed by these commitments. It is our firm belief that we must be continually vigilant and entirely committed to the on-going improvement of our security defenses because the adversaries seeking to harm infrastructure of all kinds, including natural gas pipelines, are nimble and the threats they pose are evolving.

Pipeline operators take a risk-management approach to addressing security threats

Industry security efforts seek to reduce the risk posed by a successful attack targeting our infrastructure. This risk-informed approach helps us prioritize our actions and allocate appropriate resources toward the highest priority. Pipeline operators utilize a variety of tools and resources, like the *NIST Cybersecurity Framework* and the *TSA Pipeline Security Guidelines,* to build well-rounded cybersecurity programs that effectively assess and manage the risks that we face. We recognize that cybersecurity risk management strategies must be comprehensive in nature and must implement measures to both reduce the likelihood of a successful attack and mitigate the impacts of a successful attack, should one occur. As such, pipeline operators assess their security programs using a variety of resources such as Federal assessment programs, self-assessments, peer reviews, and third-party vulnerability and penetration tests. Exercises and tabletops also play an important role in testing our security programs, sharing information with our peers about our security practices, and planning for how we will work across industry, interdependent sectors and with first responders during an incident.

A foundational element of a well-informed risk management program is comprehensive information sharing. This is a key point that deserves emphasis. Real-time, actionable information is vital to ensuring pipeline operators are equipped with the latest intelligence on threats, including known tactics, techniques, and mitigative measures. This, in turn, enables operators to evaluate their risks and tailor an approach that best fits the needs of their individual systems and environments. Strong information sharing already occurs today between INGAA member companies and other industry stakeholders through the work of our information sharing and analysis centers (ISACs), including the Downstream Natural Gas (DNG) ISAC and the Oil and Natural Gas (ONG) ISAC. However, this cannot be industry's responsibility alone. It is imperative that we also have a cooperative relationship with our Government partners to facilitate rapid information sharing. It is worth emphasizing that the pipeline industry has a strong information-sharing relationship with our partners at TSA and U.S. Department of Homeland Security (DHS). We would like to see this relationship of trust continue and develop, as we look toward these agencies to declassify threat intelligence and provide us with the timely, actionable information necessary to protect our systems and infrastructure.

The Transportation Security Administration pipeline security program is improving

The Aviation and Transportation Security Act (Pub. L. 107–71) ("ATSA") vested the Transportation Security Administration with authority over pipeline security. Pursuant to this authority, TSA offers guidance on expected practices and procedures necessary to secure the Nation's critical pipeline infrastructure. TSA offers several programs, tools, and products to assist pipeline operators with protecting their infrastructure, including Critical Facility Security Reviews, Corporate Security Reviews, Pipeline Cybersecurity Assessments, Smart Practices, I–STEP, Security Awareness Training Videos, and the International Pipeline Security Forum.

TSA acknowledges that there remains room for improvement in its pipeline security program. The agency has accepted the recommendations for improving the management of its pipeline security program that were made by the Government Accountability Office and is in the process of implementing them. INGAA strongly believes that if followed, these recommendations will help to make a stronger and more robust program.

Following the tragic events of September 11, 2001, TSA's security program was rooted in the physical security threats targeting our critical infrastructure. As acknowledged in a recent statement by Director of National Intelligence Dan Coats, sophisticated nation-state-backed cybersecurity capabilities present a real threat to our critical infrastructure. These threats have led to increased emphasis by TSA and our sector on protecting pipeline infrastructure from cybersecurity threats. It is important to stress that these threats are faced by all critical infrastructure and not just natural gas pipelines. The increasing interdependence across the segments of our Nation's critical infrastructure means that we must work together across industry and Government to protect ourselves against these threats.

The work that TSA and DHS are doing through the National Risk Management Center (NRMC) is a very positive step toward the end goal of protecting the Nation

from cybersecurity threats. These agencies are working together to understand how sophisticated, nation-state threat actors seek to identify ways to harm all U.S. critical infrastructure. We believe this approach is significant because these threats cannot be analyzed effectively in isolation. All critical infrastructure is being targeted; therefore, we must identify the best ways to work together to protect our National security.

In October, these agencies announced the Pipeline Cybersecurity Assessment Initiative, which is working to conduct comprehensive cybersecurity assessments of natural gas infrastructure to better understand the unique risks faced by our infrastructure as well as to identify how best to protect it. In addition to having a recognized baseline of practices, assessments are critical to providing assurance that these programs are working. TSA has already piloted one INGAA member assessment in 2018, and INGAA members continue to volunteer to participate in these new assessments in 2019.

Next steps for building upon progress to secure pipeline infrastructure

INGAA believes that progress has been made in securing our pipeline infrastructure and that the focus should be on continuing to improve TSA's pipeline security program. Threat actors regularly develop and refine their tactics, and we must do the same. The increased coordination between TSA and DHS's Cybersecurity and Infrastructure Security Agency (CISA) through the NRMC is an appropriate response to the enhanced need for cybersecurity expertise to support industry's efforts to protect our critical infrastructure against these growing threats. We understand TSA has embraced GAO's recommendations as a roadmap for improving its pipeline security program and is already taking steps to respond to them.

INGAA and its member companies will continue to support TSA's efforts. This includes volunteering for assessments, sharing information about indicators of compromise and about how member companies are securing their infrastructure, and participating in cross-sector exercises so we can better determine how the different segments of critical infrastructure must work together.

The growing threat of nation-state-backed attacks requires a coordinated and comprehensive approach across all critical infrastructure and across all Federal agencies supporting National security. INGAA believes that TSA's on-going work with the NRMC and CISA is bridging that gap. We urge Congress to support TSA's efforts to improve its program and to provide the necessary guidance and funding for additional program management staffing and cybersecurity expertise that can work directly with the NRMC and support the new Pipeline Cybersecurity Assessment Initiative. INGAA believes that this supplement to efforts already under way will help make TSA successful in its mission to protect the Nation's pipeline infrastructure.

Mr. CORREA. Thank you very much for your testimony.

Now I will recognize, Mr. Olson, for 5 minutes.

STATEMENT OF ERIK ROBERT OLSON, VICE PRESIDENT, RAIL SECURITY ALLIANCE

Mr. OLSON. Chairman Correa, Chairman Richmond, Ranking Member Lesko, and Members of the subcommittees, my name is Erik Olson, and I am the vice president of the Rail Security Alliance. The Rail Security Alliance is a coalition of North American freight rail manufacturers, suppliers, unions, and steel interests, committed to ensuring the economic and National security of our passenger and freight rail systems. On behalf of our coalition thank you for the opportunity to testify on the critical topic of securing our surface transportation systems against cyber and privacy threats.

With thousands of miles of railroad covering the United States, freight rail regularly transports everything from sensitive U.S. military equipment, to toxic and hazardous waste every day. On the passenger side millions of Americans rely on the commuter rail system daily. U.S. Rail System is also highly sophisticated, relying on a constantly expanding network of technology that dramatically increases its risks to cyber attack and hacking.

Today I want to draw the committee's attention to a particular threat arising from foreign investments in this industry that jeopardizes directly the future of America's Passenger and Freight Rail Systems. This threat is China.

China is strategically targeting the U.S. rail manufacturing sector with aggressive anti-competitive tactics and how do we know that? Well, to date they have secured 4 U.S. metropolitan transit contracts in Boston, Chicago, Philadelphia, and Los Angeles, largely by utilizing anti-competitive under-bidding practices. These aggressive and anti-competitive activities are not unusual for China state-owned rail sector and raise grave National concerns, security concerns that demand immediate attention.

Without decisive action America's industrial, military, and other Government interests could be forced to rely significantly or wholly on rail cars made by the Chinese government thus creating massive cyber vulnerabilities that threaten our Nation.

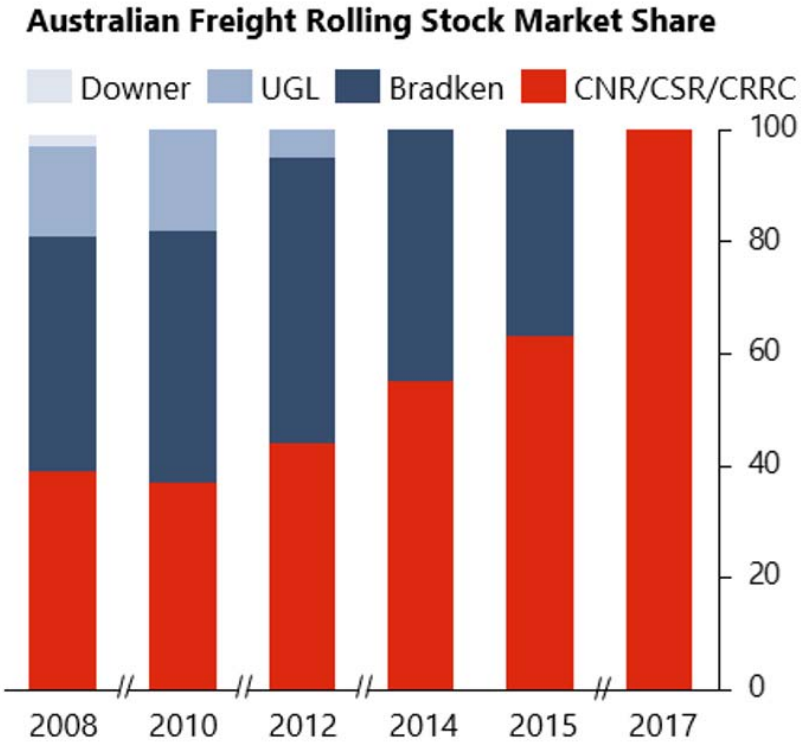
The Made in China 2025 Initiative, a key component of China's 13th 5-Year Plan identifies the rail manufacturing sector as a top target for Chinese expansion. This initiative has systematically and deliberately driven strategic investment and financing activities of the state-owned China Railway Rolling Stock Corporation, CRRC, in third-country markets and the United States. CRRC is wholly owned by the government of China. It has 90 percent of China's domestic market for production of rail locomotives, bullet trains, passenger trains, and Metro vehicles.

In just the last 5 years alone in the United States, we have witnessed CRRC execute a business strategy to take market share in the U.S. transit rail manufacturing sector deploying near-limitless financing from its home government, allowing CRRC to establish itself as a formidable force in the U.S. rail transit manufacturing base.

Emboldened with these contract victories, CRRC continues to target other U.S. cities including our Nation's capital. In September the Washington Metropolitan Transit Authority, WMATA, issued a request for proposal for the new 8000-series Metro Car. This RFP includes numerous technologies which are susceptible to cyber attacks. Whoever is selected to supply rail cars for WMATA will become a partner in the day-to-day operations of a Metro System whose stops include the Pentagon, the Capitol, as well as unfettered access to D.C.'s tunnels and underground infrastructure. As CRRC itself has stated, their objective is to conquer the rest of the global rail market—need I say more? Whether they be State, local, or Federal funds, American taxpayer dollars should not be used to subsidize the activities of a Chinese state-owned enterprise and compromise American security.

Based on the experiences of Australia, which this graph denotes, whose domestic industry, CRRC was able to wipe out in under a decade, we are equally concerned that CRRC will leverage its growing presence in the U.S. transit rail production to then pivot into freight rail assembly; we cannot allow this to happen here.

[The information follows:]



Source: Oxford Economics; RSA internal data

Mr. OLSON. Yet the Department of Homeland Security deems the U.S. rail sector as a part of the Nation's critical infrastructure, running through every major American city and every military base in the Nation. We have had extensive discussions with representatives from DOD and based on those discussions, I am confident that the Secretary of Defense will express his concerns on this matter as well.

As China's CRRC becomes more dominant [inaudible] should the United States rely on a Chinese state-owned enterprise for the production of our countries freight and passenger rail cars, the position of RSA is a resounding, no. The strategic targeting of our Nation's infrastructure by the government of China and its state-owned enterprises poses a fundamental threat to the fabric of our critical infrastructure and is a pressure point for malicious cyber actors to threaten not only the economic and National security of the United States but our standing as a global power.

Thank you again for the opportunity to testify. I look forward to answering any questions you may have.

[The prepared statement of Mr. Olson follows:]

PREPARED STATEMENT OF ERIK ROBERT OLSON

FEBRUARY 26, 2019

INTRODUCTION

Chairman Correa, Chairman Richmond, Ranking Member Lesko, Ranking Member Katko, and Members of the subcommittees, my name is Erik Olson and I am the vice president of the Rail Security Alliance. The Rail Security Alliance is a coalition of North American freight rail car manufacturers, suppliers, unions, and steel interests committed to ensuring the economic and National security of our passenger and freight rail systems. On behalf of our coalition, thank you for the opportunity to testify on the critical topic of securing our surface transportation systems against cyber and privacy threats.

Rail in the United States is an integral component of our critical infrastructure and our way of life. With nearly 140,000 miles of railroad covering the United States, freight rail regularly transports key commodities, sensitive U.S. military equipment, hazardous waste, potentially toxic and hazardous chemicals, and flammable liquids across the country every day. On the passenger side, millions of Americans rely on commuter rail systems every day. The U.S. rail system is also highly sophisticated, relying on a constantly expanding network of technology and digitization that dramatically increases its risk to cyber attack and hacking.

Today, I want to draw the committee's attention to a particular threat arising from foreign investment in this industry that jeopardizes the future of America's passenger and freight rail systems. China is strategically targeting the U.S. rail manufacturing sector, with aggressive, strategic, and anticompetitive actions. Thus far they have secured four U.S. metropolitan transit contracts, largely by utilizing anticompetitive under-bidding practices. With China's government picking up U.S. transit rail manufacturing contracts, the Chinese are now using their rail manufacturing capabilities to assail the U.S. freight manufacturing sector in a move that is reminiscent of what has already occurred in third-country markets such as Australia. This activity is a pattern for China's state-owned rail sector and raises grave National security concerns. Without action, America's industrial, military, and other Government interests could be forced to rely significantly or wholly on rail cars made by the Chinese government, thus creating massive cyber vulnerabilities that threaten our military and industrial security.

CHINA'S STATE-OWNED ENTERPRISES TARGET U.S. RAIL MANUFACTURING

The "Made in China 2025" initiative, a key component of China's 13th Five-Year plan,[1] identifies the rail manufacturing sector as a top target for Chinese expansion. This initiative has systematically and deliberately driven strategic investment and financing activities of the state-owned China Railway Rolling Stock Corporation (CRRC) in third-country markets and the United States. CRRC is wholly owned by the government of China and it has 90 percent of China's domestic market for production of rail locomotives, bullet trains, passenger trains, and metro vehicles.[2] In 2015, CRRC reported revenues of more than $37 billion[3]—significantly outpacing the entire U.S. rail car market, which had $22 billion of output during the same year.[4] According to Chinese state media, CRRC plans to increase overseas sales to $15 billion by next year alone. This represents about double the level of export orders from just 4 years ago[5] and according to CRRC's own presentation materials the U.S. market remains a prime target to, as they put it, "conquer."[6]

Using State-backed financing, subsidies, and an array of other government resources, CRRC has strategically targeted and sought to capture the U.S. railcar

[1] U.S.-China Economic and Security Review Commission, *2016 Report to Congress,* November 2016, at 100.

[2] Langi Chiang, *China's largest train maker CRRC Corp announces 12.2 billion yuan in contracts,* South China Morning Report, July 23, 2015. *https://www.scmp.com/business/companies/article/1842983/chinas-largest-train-maker-crrc-corp-announces-122-billion-yuan.*

[3] CRRC Corporation, 2015 CRRC Annual Report, *https://www.crrcgc.cc/Portals/73/Uploads/Files/2016/8-23/636075436968234671.pdf.*

[4] Oxford Economics, *Will We Derail US Freight Rolling Stock Production?,* May 2017, at 24.

[5] Brenda Goh, *China Trainmaker CRRC to build more plants abroad in expansion plan: China Daily,* REUTERS, Dec. 5, 2016, *http://www.reuters.com/article/us-crrc-expansion-idUSKBN13U0EJ.*

[6] @CRRC_global, "Following CRRC's entry to Jamaica, our products are now offered to 104 countries and regions. So far, 83 percent of all rail products in the world are operated by #CRRC or are CRRC ones. How long will it take for us conquering the remaining 17 percent?" Twitter, January 11, 2018. *https://twitter.com/CRRC_global/status/951476296860819456.*

manufacturing sector. In just the last 5 years the United States has witnessed CRRC establish rail assembly operations for transit railcars in 3 States, along with additional research and bidding operations in several others. By beginning with a business strategy to take market share in the U.S. transit rail manufacturing sector and deploying near-limitless financing from its home government to help lower the well-below-market bids for new U.S. metropolitan transit projects, CRRC has quickly established itself as a formidable force in U.S. transit rail competition.

Several recent cases involving CRRC bids for new transit rail projects serve as compelling examples of the strategy being employed by China to capture our rail systems:

- CRRC bid $567 million to win a contract with the Massachusetts Bay Transit Authority (MBTA) in Boston in 2014, coming in roughly 50 percent below other bidders.[7]
- In 2016, CRRC won a contract to provide transit rail for the Chicago Transit Authority (CTA), bidding $226 million less than the next-highest bidder.[8]
- In early 2017, CRRC bid $137.5 million for a contract with Southeastern Pennsylvania Transportation Authority (SEPTA) in Philadelphia, underbidding the next-lowest bidder—which had a robust local manufacturing presence—by $34 million.[9]
- In March 2017, CRRC finalized a contract with the Los Angeles County Metropolitan Transportation Authority for its transit rail system worth up to $647 million.[10] Again, China did this by leveraging below-market financing, which in turn undercut other bidders.

Emboldened with these contract wins, CRRC continues to target other U.S. cities, including our Nation's capital. In September, the Washington Metropolitan Transit Authority (WMATA), which is the second-largest mass transit system in the country, issued a Request for Proposals (RFP) for the new 8000-series metro car. This RFP includes video surveillance, monitoring and diagnostics, data interface with WMATA, and automatic train control systems that are susceptible to cyber attacks. In response to concerns expressed by a number of lawmakers, including the Vice Chairman of the Senate Intelligence Committee, WMATA re-issued its RFP to include additional cybersecurity protections.[11]

But the Rail Security Alliance's concerns do not end there. Whomever is selected to supply rail cars for WMATA will become a partner in the day-to-day operations of a Metro system whose stops include the Pentagon and the Capitol, as well as unfettered access to our Nation's tunnels and underground infrastructure.

We couple this reality with two additional critical facts. First, a Classified report written by WMATA's inspector general recently concluded that there were significant shortcomings in WMATA's enterprise-level cybersecurity posture.[12] Second, just last week the *New York Times* noted that "businesses and government agencies in the United States have been targeted in aggressive attacks by . . . Chinese hackers . . . ".[13] So, in light of China's pervasive history of cyber espionage and hacking, it is the position of the Rail Security Alliance that we cannot trust a Chinese state-owned enterprise to build, own, or operate in U.S. critical infrastructure.

These developments are even more alarming because they provide CRRC the opportunity to pivot into freight rail assembly, a subsector of rail not protected by the

---

[7] Bonnie Cao, *After Winning MBTA Contract, China Trainmaker CRRC Plans American Expansion,* Boston Globe, Sept. 11, 2015. *https://www.bostonglobe.com/business/2015/09/11/after-winning-mbta-contract-china-trainmaker-crrc-plans-american-expansion/jnS1kU7uHWFGR9gjWmDEjM/story.html*.

[8] Corilyn Shropshire, *First Step to New CTA Rail Cars: Build the Factory in Chicago,* Chicago Tribune, Mar. 16, 2017. *http://www.chicagotribune.com/business/ct-cta-new-railcar-plant-0316-biz-20170315-story.html*.

[9] Jason Laughlin, *Mass.-Based Company with Chinese Backing Beats Local Group for SEPTA Car Contract,* The Philadelphia Inquirer, Mar. 21, 2017. *http://www.philly.com/philly/business/transportation/Mass-based-company-with-Chinese-backing-beats-out-local-group-for-SEPTA-car-contract.html*.

[10] Keith Barrow, *Los Angeles Orders CRRC Metro Cars,* International Railway Journal, Mar. 24, 2017. *http://www.railjournal.com/index.php/north-america/los-angeles-orders-crrc-metro-cars.html*.

[11] Sean Lyngaas, D.C. Metro system beefs up supply chain cybersecurity provisions for new rail cars, Cyberscoop, February 6, 2019. *https://www.cyberscoop.com/metro-dc-subway-cyberscecurity-rfp/*.

[12] Ryan Johnston, *D.C. Metro needs to improve its cybersecurity, audit finds,* Statescoop, July 9, 2018. *https://statescoop.com/wmata-incident-response-audit-calls-for-improved-cybersecurity-plan/*.

[13] Nicole Perlroth, *Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies,* New York Times, February 18, 2019. *https://www.nytimes.com/2019/02/18/technology/hackers-chinese-iran-usa.html*.

same Buy America requirements as transit rail, and one that represents a troubling vulnerability if overtaken by the government of China. Even so, CRRC is making steady and deliberate headway into this sector with the launch of Vertex Rail Corporation and American Railcar Services. Vertex Rail Corporation is now, a defunct freight rail assembly facility that was based in Wilmington, North Carolina. On the other hand, American Railcar Services is a separate assembly facility headquartered in Miami, FL that maintains assembly operations in Moncton, New Brunswick.

Concerns about CRRC's transition into freight rail manufacturing are best illustrated by the recent experiences of third-country markets like Australia, whose freight rail manufacturing sector CRRC entered in 2008. In less than 10 years, CRRC effectively decimated the sector, forcing the 4 domestic suppliers out of business and out of the rail market which left only CRRC standing. Today, almost no meaningful Australian passenger or freight rolling stock manufacturing exists—CRRC's Australia footprint is almost exclusively that of an assembler of Chinese-made parts and a financier of purchases from CRRC. We cannot let that happen here.

IMPLICATIONS FOR NATIONAL SECURITY

Unlike the U.S. maritime shipping industry, whose security is protected by the Jones Act, a measure that requires vessels transporting goods between U.S. ports to be U.S.-built and majority U.S.-owned, freight rail in America has been left comparatively unprotected. Yet, the Department of Homeland Security (DHS) deems the

U.S. rail sector as part of the Nation's critical infrastructure,[14] noting that 140,000 rail miles enable U.S. freight rail to run through every major American city and every military base in the Nation. The Department of Defense (DoD), which itself maintains a fleet of more than 1,300 rail cars, has also designated nearly 40,000 miles of freight rail as part of the Strategic Rail Corridor Network (STRACNET), a comprehensive rail network that connects military bases and maritime ports across the country.[15] We have had extensive discussions with representatives from the Department of Defense, and based on those discussions I am confident that the Secretary of Defense would express his concerns on this matter as well.

Because freight rail transports not only military freight and industrial products, but also nuclear material and hazardous chemicals that can be safely and effectively transported only by rail, there is a serious risk that the technologies in these systems could be compromised by a malicious actor. As noted by Brig. Gen. John Adams (USA, Ret.) in a 2018 report on the vulnerabilities of freight rail,[16] our rail system's rapidly expanding internet of things (IoT) capabilities presents an array of National security challenges that include:

- *A digitized railroad network/the internet of things*.—Integrated teams of data scientists, software developers, and engineers develop and apply technology across every aspect of the Nation-wide freight rail network, effectively increasing the vulnerability of industrial control systems, train operations, and perhaps even the industry's metadata warehousing centers to cyber threats.
- *Rail Signaling*.—Congress has mandated the installation of positive train control (PTC) systems on much of the Nation's rail systems as a means of preventing specific accidents. A malicious cyber breach of PTC or underlying existing rail signaling systems could wreak havoc and cause accidents or derailments on the highly interdependent freight railway network.
- *Locomotives*.—Rail locomotives rely upon hundreds of sensors to monitor asset health and performance of train systems.
- *On-board Freight Car Location & Asset Health Monitoring*.—Thousands of freight cars are equipped with telematics or remote monitoring equipment, many of which are carrying hazardous materials like chlorine, anhydrous ammonia, ethylene oxide, and flammable liquids. This tracking technology includes a wireless communication management unit to track precise near-real-time location via GPS, direction of travel, speed, and dwell time within the Transportation Security Administration (TSA)'s 45 designated high-threat urban areas (HTUAs).[17]

End-of-Train Telemetry (EOT).—The FRA requires all freight trains operating on excess of 30 mph to be equipped with a 2-way EOT device that tracks GPS location and can allow a locomotive engineer to initiate an emergency brake application, a critical safety feature for trains that can stretch upwards of 10,000 feet long (See Attachment A).

The presence of these evolving technologies underscores the clear danger of a foreign country, and particularly the government of China and its state-owned enterprises, having undue control of freight manufacturing in the U.S. market. Already, there are reports of Chinese manufacturers investigating the production of their own "telematics" technology to allow the monitoring and control of their rail cars.[18] On the transit side, China is already boasting about how it has utilized the latest advances in AI and facial recognition technology to identify and track its 1.4 billion citizens,[19] creating a very real prospect that they could do the same here in the United States.

---

[14] Presidential Policy Directive 21 (PPD–21) identifies 16 critical infrastructure sectors, including "Transportation Systems." The Department of Homeland Security defines "Freight Rail" as 1 of the 7 key subsectors. See generally, PPD–21, *Critical Infrastructure Security and Resilience,* Feb. 12, 2013, *https://www.whitehouse.gov/the-press-office/2013/02/12/Presidential-policy-directive-critical-infrastructure-security-and-resil* and Transportation Systems Sector, Dep't of Homeland Sec., Mar. 25, 2013, *http://www.dhs.gov/transportation-systems-sector.*

[15] "Strategic Rail Corridor Network (STRACNET)," Global Security, 2012. *https://www.globalsecurity.org/military/facility/stracnet.htm*.

[16] National Security Vulnerabilities of the U.S. Freight Rail Infrastructure and Manufacturing Sector—Threats and Mitigation, Brigadier General John Adams, US Army (Retired), October 22, 2018.

[17] The Transportation Security Administration defines an HTUA as an area comprising one or more cities and the surrounding areas, including a 10-mile buffer zone.

[18] *China plans "smart trains" to take on global rail companies,* CHINA DAILY, March 10, 2016, *http://english.chinamil.com.cn/news-channels/2016-03/10/content_6952271_2.htm.*

[19] *Surveillance Cameras Made by China Are Hanging All Over the U.S.,* The Wall Street Journal, November 12, 2017. *https://www.wsj.com/articles/surveillance-cameras-made-by-china-are-hanging-all-over-the-u-s-1510513949*.

CONCLUSION

As China's CRRC becomes more dominant as a U.S. rail manufacturer, there are urgent and compelling questions we must answer regarding whether a growing presence of, and reliance upon freight or passenger cars from a major state-owned Chinese rail enterprise is likely to compromise the security and safety of industrial, military, and civilian transportation systems in the United States. For that reason, we are grateful that Congress passed legislation last year that would mandate the Department of Homeland Security, in coordination with the Committee on Foreign Investment in the United States and the Department of Transportation, produce a report on the National security threats of Chinese SOE investment in our rolling stock manufacturing sector,[20] and we strongly urge the committee to work with DHS as that report is completed.

We greatly appreciate the committee's interest in addressing these critical issues. The strategic targeting of our Nation's infrastructure by the government of China and its state-owned enterprises poses a fundamental threat to the fabric of our critical infrastructure and is a pressure point for malicious cyber actors to threaten not only the economic and National security of the United States, but to our standing as a global power.

Thank you again for the opportunity to testify. I look forward to answering any questions you may have.*

Mr. CORREA. Thank you, for your statements.

I would like to recognize Mr. Hultquist, for 5 minutes.

STATEMENT OF JOHN HULTQUIST, DIRECTOR OF INTELLIGENCE ANALYSIS, FIRE EYE

Mr. HULTQUIST. Chairman Correa, and, Ranking Member Lesko, for convening this joint hearing today. My name is John Hultquist, and I am the director of intelligence analysis for FireEye. My team of over 150 intelligence analysts and researchers pore over data we collect from FireEye's global networks of devices, incident response, researchers monitoring the criminal underground and many more sources to understand the global cyber threat.

FireEye is supporting the transportation and energy sectors here at home. We are protecting TSA with email—thank you—and web inspection and we are providing support to DHS's subscription to our intelligence reporting.

At DOE we are supporting network and file inspection, malware analysis, and protecting their data from threats down at their endpoints. The Department is the largest civilian agency, consumer of our intelligence reporting which provides focused visibility into threats targeted at the energy sector.

Today I will focus primarily on threats on the horizon that FireEye is watching develop in the Middle East, Ukraine, South Korea, where Iran, Russia, North Korea, are the most active.

Despite a dearth of recent specific examples of pipeline targeting by state actors that we have observed, targeting the sector is consistent with the behavior of several state actors who have carried out disruptive and destructive operations. Pipelines sit at the nexus of two well-established interests for state actors, energy and transportation. For example, oil and gas has been the major focus of a long-term destructive malware campaign by Iran in the Gulf.

Though these attacks have targeted critical infrastructure organizations, they have primarily affected business-focused IT systems

[20] See. H.R. 5515—John S. McCain National Defense Authorization Act for Fiscal Year 2019, Sec. 1719(c).

*Attachment A has been retained in committee files and is available at *https://go.americanmanufacturing.org/page/-/Adams__Freight__Rail.pdf.*

rather than sensitive controls systems. Nonetheless Iranian-sponsored threat actors have caused significant, costly disruptions from 2012 to as recently as 2018 using this capability.

The Middle East was also the scene of the most disconcerting attack on control systems we have observed. In an industrial plant, they have suffered a disruption when attackers inadvertently triggered a shutdown using a malware we call Triton. They triggered the shutdown because they were attempting to manipulate automated safety systems, one of the last lines of defense to protect human life. We believe this activity originated from a Russian government organization.

Transportation and logistics systems have been unrecognized but fruitful focus for state cyber attackers as well. During and between attacks on Ukraine's grid, attempts were made by the same Russian actors to gain access to rail, air, and sea transportation routes and hubs to varying degrees of success.

Many of the companies which posted major losses from the NotPetya Ransomware incident in the hundreds of millions of dollars were also in the logistics business, despite this industry not having been specifically targeted. Such a pattern could indicate that logistics organizations may be especially economically vulnerable to incidents of this nature.

Like pipeline operations, transit networks have been subjected to ransomware operations and denial-of-service attacks which have on occasions resulted in disruption to service. Ransomware which has affected many municipal services has been used to hold transit systems hostage in return for payment. The websites associated with mass transit systems which are often crucial to their business have also been subjected to denial-of-service attacks, in some cases disrupting travel. Both ransomware and denial-of-service are capabilities used by state actors.

The complexity of transit networks and the potential for cascading economic consequences from disruption, bear similarities to pipelines, however transit networks offer an additional attraction to would-be attackers. Transit is a highly-visible sector with which the public regularly interacts; this factor is especially relevant as many cyber attacks appear to be more focused on psychological effects and undermining confidence in institutions and creating lasting physical effects.

It is important to bear in mind that our adversaries are not necessarily preparing for a doomsday situation or any lasting blow but a asymmetric scenario where they can project power onto our shores. Ultimately their aim may be to sow chaos rather than to achieve some complex military objective.

Thank you, again for the opportunity to participate in today's discussion. I am happy to answer any of your questions.

[The prepared statement of Mr. Hultquest follows:]

PREPARED STATEMENT OF JOHN HULTQUIST

FEBRUARY 26, 2019

Thank you, Chairman Richmond, Ranking Member Katko, Chairman Correa, and Ranking Member Lesko for convening this joint hearing today. We appreciate the opportunity to share FireEye's perspective on threats to the transportation and en-

ergy sectors and provide an overview of how the private sector is helping to secure those sectors.

INTRODUCTION

My name is John Hultquist, and I'm the director of intelligence analysis for FireEye. My team of over 150 intelligence analysts and researchers pore over data we collect from FireEye's global networks of devices, managed defense of 7 global Security Operations Centers, our incident response, researchers we have monitoring the criminal underground, and many more sources to understand the global cyber threat. We have teams focused on criminal threats, cyber espionage, cyber physical, and strategic problems, as well as vulnerabilities. Ultimately, we provide intelligence reporting and services used by Government and commercial clients around the world.

In addition to the 300-plus security professionals responding to computer intrusions, FireEye has over 200 cyber-threat analysts on staff in 18 countries, speaking 30 different languages, to help us predict threats and better understand the adversary—often by considering the political and cultural environment of the threat actors. We have an enormous catalog of threat intelligence, and it continues to grow everyday alongside the continually increasing attacks on organizations around the world.

FireEye is supporting the transportation and energy sectors here at home. We're protecting the Transportation Security Administration with both email and web inspection, managed by the Department of Homeland Security's Enterprise Security Operations Center. As TSA continues to stand up its intelligence capabilities, we are providing support through its subscription to our intelligence reporting.

Additionally, we assist in protecting the Department of Energy by supporting network and file inspection, malware analysis, and protecting their data from threats down to their endpoints. We provide the ability for deep forensics inspection of all network traffic managed by the Department's Enterprise Security Operations Center. As DOE continues to enhance its cyber capabilities, we provide visibility to meet the Data Taxonomy Metrics. The Department is the largest civilian agency consumer of our intelligence reporting, which provides focused visibility into the threats targeted at the energy sector.

In addition to my role at FireEye I'm an adjunct professor at Georgetown University and the founder of CYBERWARCON, a conference on the cyber attack and information operations threat.

I have been working in cyber intelligence for over a decade, most of it at FireEye, but before that I worked as a contract cyber intelligence analyst with the Defense Intelligence Agency and State Department. Prior to that I worked briefly at the Surface Transportation and Public Transit Information Sharing and Analysis Center where I was an analyst exploring threats to the sector we will be discussing today. Part of my duties there were to forecast domestic threats by exploring global incidents. Though much of this work was focused on counterterrorism, I believe the methodology I employed there is applicable to this problem. If we want to forecast threats to surface transportation, we have to look globally for the actors who may target this sector, and explore not just how they carry out attacks, but why.

Today I will talk about a few incidents that have already affected surface transportation, but I will focus primarily on threats on the horizon that FireEye is watching develop in the Middle East, Ukraine, and South Korea, where Iran, Russia, and North Korea are most active. My team has had some success with this method. In 2014, we exposed an actor, who we call Sandworm Team, which was carrying out cyber espionage in Ukraine and who was soon after exposed in U.S. critical infrastructure. A year later this actor caused the first known blackout by cyber attack in the Ukraine.

PIPELINES

Criminal, state, and hacktivist actors have all demonstrated an interest in pipeline operators. Pipeline operators have been the victim of criminal ransomware incidents on multiple occasions. Hacktivist actors have threatened pipelines for environmental and other political reasons. We have seen some specific interest in pipeline infrastructure from state actors as well. APT1, an actor tied to China's People's Liberation Army, carried out an intrusion campaign attempting to gain access to pipeline operators in 2012. While we do not think the campaign aimed to cause any immediate effects, at the time we did assess that it was reconnaissance of our infrastructure that could be leveraged over the long term.

Despite the dearth of additional specific examples of pipeline targeting, targeting the sector is consistent with the behavior of several state actors who have carried

out disruptive and destructive operations. Pipelines sit at the nexus of two well-established interests for these state attackers: Energy and transportation. Despite a relatively brief history of disruptive and destructive cyber attacks against critical infrastructure, several incidents have focused on these sectors where the potential for cascading economic and psychological effects on the target population is considerable.

Energy, particularly oil and gas and the electrical power industry, has been the continued focus of threat actors who have either carried out disruptive cyber attacks or who appear to be tasked with preparing for such an operation. Destructive and disruptive attacks on oil and gas have almost become common in the Middle East where our U.S. adversaries are showcasing their capabilities and improving their skills.

For example, oil and gas has been the major focus of a long-term destructive campaign by Iran in the Gulf using destructive malware commonly referred to as "Shamoon." Though these attacks have targeted critical infrastructure organizations, they have primarily affected business-focused IT systems rather than the sensitive control systems which run production. Nonetheless, Iranian-sponsored threat actors caused significant, costly disruptions from 2012 to as recently as December 2018, the last time we observed one of these incidents.

The Middle East was also the scene of the most disconcerting attack on control systems we have observed. An industrial plant there suffered a disruption when attackers inadvertently triggered a shutdown using malware we call TRITON. They triggered that shutdown because they were attempting to manipulate automated safety systems, one of the last lines of defense to protect human life. We believe the attackers were developing the ability to create an unsafe condition using the control systems, while simultaneously disabling the safety systems designed to mitigate the attack. Such a scenario could have led to major disruption of operations, economic loss, and even loss of life. We believe this activity originated from a Russian government organization called the Central Scientific Research Institute of Chemistry and Mechanics. It is unknown whether these actors had been tasked to target the plant for some specific geopolitical goal or if they were using this Middle Eastern facility as a testbed to improve their capability.

In principal, methodologies honed in the Middle East against oil and gas could be applied to our pipeline sector. Destructive attacks could be used to interrupt the administration of these complex systems, potentially causing economic repercussions that cascade through the myriad of downstream users who depend on reliable service. A more complex scenario, like the TRITON incident, could also target pipelines, which could be manipulated to potentially disastrous consequences if actors can gain access to control and safety systems.

Transportation and logistics systems have been an underrecognized but fruitful focus for state cyber attackers as well. During and between well-known attacks in Ukraine which turned off the power to portions of the country, attempts were made by the same Russian actors to gain access to rail, air, and sea transportation routes and hubs, to varying degrees of success. In fact, we saw evidence indicating that while they were prepping the first attack that briefly disabled power service in the Ukraine, the actors we call Sandworm Team were also compromising airport and rail services. There are plausible but unverified reports of an attack which lead to disruption of rail service coincided with the second attack on Ukraine's grid.

As in the case of the Middle East, in Ukraine, we see technically complex cyber attacks that strike at the most sensitive industrial control systems, such as those that caused blackouts, as well as attacks that are not focused on these systems at all. Both types of attack have been successful. While grid attacks were undoubtedly watershed events, the most economically damaging attack we have ever encountered was fake ransomware called NotPetya. This fake ransomware-encrypted drives just like its real criminal counterpart, but the state actors behind it never intended to decrypt this information for any amount of money, essentially making it a destructive tool. The malware spread rapidly, locking up vital systems and causing major disruptions to global companies. The result was over 10 billion dollars in damages, according to one White House estimate. Most notably, however, many of the companies which posted major losses in the hundreds of millions were in the logistics business, despite this industry not having been specifically targeted. Such a pattern could indicate that logistics organizations may be especially economically vulnerable to cyber attacks of this nature.

TRANSIT

Like pipeline operations, transit networks have been subjected to ransomware operations and denial-of-service attacks, which have, on occasion, resulted in disrup-

tion to service. Ransomware, which has affected many municipal services, has been used to hold transit systems hostage in return for payment. An attack like this in San Francisco took tickets systems off-line, but operations continued when riders were offered free passage. In most cases we believe the attackers were financially motivated, though it is worth noting that these incidents expose a vulnerability that state actors, who have used a fake ransomware capability, could exploit.

In addition to ransomware incidents, the websites associated with mass transit systems, which are often crucial to their business, have been subjected to denial-of-service attacks. These incidents, which involve the use of a network of hijacked computers to jam a website with bogus traffic, have in some cases frozen operations. We have seen this phenomenon as far afield as Ukraine and Sweden. In 2017, transit systems in Sweden came under a prolonged attack by an unknown actor who disrupted travel. It is worth noting that like ransomware, denial of service is a capability used by state actors. And just as ransomware allows these actors to carry out attacks while hiding their true intentions, state actors have purported to be hacktivists and taken credit for denial-of-service attacks, hiding their hand it the operations. This was the case in the United States, where Iranian hackers attacking our financial system claimed to be a pan-Arab hacktivist. Furthermore, there is a reduced barrier to entry for these types of attacks, and even states without this capability could source it from the criminal underground.

The complexity of transit networks and the potential for cascading economic consequences from disruption bear similarities to pipelines; however, transit networks offer an additional attraction to would-be attackers—transit is a highly-visible sector with which the public regularly interacts. This factor is especially relevant as many cyber attacks appear to be more focused on psychological effects and undermining confidence in institutions than creating lasting physical effects.

One example of a highly-visible cyber attack which affected the populace is the destructive campaign against South Korean media and banking in 2013. Though this campaign failed to interrupt broadcasts, it did interrupt some banking services, including on-line banking and ATMs. The result was a visible crisis that affected the everyday lives of South Koreans and which might have been even greater if broadcasts were halted. Blackouts fall into this same category of having far-reaching psychological effects. A disruption to transit could have a similar effect.

CONCLUSION

Thus far, U.S. critical infrastructure has been probed by actors from China, Russia, Iran, and North Korea. In many cases, these actors have focused heavily on electricity generation; however, our experience with them abroad suggests a much broader interest in creating disruptive or destructive effects. We should take these lessons to heart now and prepare for incidents across the transportation sector.

It's important to bear in mind that our adversaries are not necessarily preparing for a doomsday situation, or any lasting blow, but an asymmetric scenario where they can project power within our shores. Ultimately, their aim may be to sow chaos rather than achieve some complex military objective. Nonetheless, these incidents could have economic and psychological effects we cannot ignore.

Thank you again for the opportunity to participate in today's discussion. And thank you for your leadership improving cybersecurity in the transportation and energy sectors. I look forward to working with you to strengthen the partnership between the public and private sectors and to share best practices to thwart future cyber attacks.

Mr. CORREA. I thank our panelists for their testimony.

If I may, I would like to recognize myself for 5 minutes of questions. I will start out with, Mr. Lewis, you made a comment at the end of your statement about credible threat, we need to be a credible threat, can you explain that a little bit?

Mr. LEWIS. Certainly. Thank you, Mr. Chairman.

When we look at the behavior of Russia, China, Iran and to some extent North Korea, they are the most dangerous attackers but they are also very calculating, they are very rational and they ask themselves, "If I do this to the Americans, what is the likelihood that the Americans will do something back?" and if they believe there is no risk that we will do anything back, they are more likely to undertake some sort of hostile or coercive action.

Mr. CORREA. In this committee last year, the full Committee on Homeland Security, I asked the question, at what point does a cyber attack constitute a declaration of war on the United States? Any thoughts?

Mr. LEWIS. This is [inaudible] was an attack that caused death or destruction or casualties, it would qualify as justifying a forceful response. Unfortunately, we haven't seen very many of them and if you look at what the Russians did in 2016, it wouldn't fall under that category so this is something that I believe the intelligence community and cyber command are working through. We need a new framework, if you cause death or destruction, you fear a risk, that you fear that the United States will retaliate. If you don't do that, people kind-of feel like they can get away with it.

Mr. CORREA. If you threaten our democracy or destabilize our Government, is that an act of war and I would ask that question to all of you?

Mr. LEWIS. Under the current legal construct, the answer would be no, right. You could make a case that by threatening the political integrity of the United States, it would qualify as an act of war but our main problem is that we became aware this was happening in April 2016, that is almost 3 years ago and we still have not done very much back.

Mr. CORREA. Mr. Olson, you talked a little bit about the challenge of Chinese assets, Chinese buying essentially their way into our markets, they are buying their markets and you talk about a threat, could you relate that back to the China's new 27 intelligence law that compels companies, Chinese companies to cooperate with the Chinese government?

Mr. OLSON. Sure. So I am not fully familiar with the law itself, I mean, I have read articles about it. I mean, our concern is that this is a wholly-owned, state-owned enterprise that has a board of directors with members of the Communist Party and we know that when they set up shop here in United States that we believe they are been directed by Beijing and the cyber issues, privacy issues, and just the economic security that stems from that is our main concern from RSA's point of view.

Mr. CORREA. Same question, to Mr. Hultquist.

Mr. HULTQUIST. Right, I am not familiar with that exact regulation but it is not uncommon for Russia or China to enforce or compel companies to work with their cybersecurity or their Signals Intelligence agencies to gather information.

Mr. CORREA. Thank you very much.

I am going to yield the remainder of my time.

I will now recognize the gentle person from Arizona, Mrs. Lesko.

Mrs. LESKO. Thank you, Mr. Chairman.

My first question is for, Mr. Hultquist, hello sir. I have a couple of questions into one. Basically, how well do you think the industry uses ISAC, the information you know, where you share information with the industry [inaudible] and my secondary question is, what are the risks from insider threats?

Mr. HULTQUIST. I had actually previously worked at a couple of the ISACs, actually the Surface Transportation and Public Transit ISAC, I worked there briefly before moving into the cyber world. They have made a lot of great strides in the cyber space and sev-

eral of them I think on are very, very mature and are making a big difference.

On one of the problems though is that we sometimes take this myopic view of our sector and we have failed to see threats coming because we are overly focused on just our own sector and it is important to look at our own sector but the actor who turned off the lights in Ukraine, was also targeting air, and rail, and all these other sectors, not because the lights were you know, particularly [inaudible] sometimes if we you know, we focus too much that way, we can kind-of miss that.

I am sorry, your second question.

Mrs. LESKO. Was, what is the risk of insider threats, like people that are working for, let us say, the rail system or passenger rail?

Mr. HULTQUIST. Many of the——

Mrs. LESKO. Or pipelines?

Mr. HULTQUIST. Major critical infrastructure incidents that we have seen throughout history have involved an insider component, a contractor who didn't get hired on was upset about their situation and decided to lock things up or I believe there was a situation where they pumped toxic stuff into a [inaudible] critical infrastructure.

Mrs. LESKO. What can be done about it, do you think?

Mr. HULTQUIST. Probably a more complex or a more robust vetting process and recognition that when people move in and out of an organization, security measures need to be sort-of re-looked at particularly do they still have access, things of that nature.

Mrs. LESKO. Thank you, sir.

My next question is for the gentleman with the rail system and you had mentioned—I read this article that I think it was in *The Washington Post,* entitled, "Could a Chinese-made Metro Car, spy on us?" I think you were quoted in this and some of the transit authorities in this article, the Chicago Transit Authority, the Massachusetts Bay Transportation Authority, they basically said that none of the critical software components were being produced in China.

What are your thoughts on that, are they misspoken or you know, they said that they are considering bids from CRRC but that the critical software components are not made in China and in fact one of the Massachusetts Bay Transportation Authority spokesman said, "The design process for new rail cars includes a cybersecurity analysis based on the U.S. Department of Defense Military System Safety Standard," so I am glad that we are bringing this up because I think it is a legitimate concern but it seems like at least from these people, spokesman, that the critical infrastructure is not made in China.

Can you comment?

Mr. HULTQUIST. Yes. What I would say to that is that our concern is you can try to mitigate and the we heard from Ms. Proctor, earlier that the cyber concerns are ever-evolving. I don't know all the parts or the list of the parts but many parts are being made in China, the shells for Los Angeles and for Boston are being made in China and shipped to Springfield, Massachusetts so our position at RSA's risk avoidance.

We don't know what can be put into a shell. We don't know what technology can be hid in there. The Chinese have a long view [inaudible] attack but we also think of it from a point of privacy. When you have access to the tunnel [inaudible] the CCTV, can you get access to the Wi-Fi system? We know how they profile their own citizens and it does not take a lot to lead to the fact that maybe you could do that here especially in the Metro region.

Mrs. LESKO. Thank you, sir.

I yield back my time.

Mr. CORREA. Thank you, Mrs. Lesko.

I recognize the gentleman from Louisiana, Chairperson Richmond.

Mr. RICHMOND. Thank you, Mr. Chairman.

This will be for Ms. Gagliostro and Mr. Olson. It is basically describing your relationship with TSA–DHS as a whole but TSA and CISA. Has there been rail stakeholder involvement in the implementation and the goals outlined in the Pipeline Cybersecurity Initiative and, Mr. Olson, in your view, are DHS and TSA being proactive enough in sharing information about cyber threats and best practices within rail systems, and to both of you all, what could they be doing differently or more?

Ms. GAGLIOSTRO. So I would say that yes, there has been rail stakeholder involvement beyond the efforts of the Pipeline Cybersecurity Initiative because as you know, that Initiative was only announced in October but prior to that TSA has been working to build its security program for over a decade now, has a very strong working relationship with industry. We regularly engage in Pipeline Sector stakeholder calls to share information about threat indicators that they are getting and also information about the tools that they are providing to industry to help us with their security programs.

I think that the work that TSA is doing right now to have more coordination with DHS and the CISA Office, and the National Risk Management Center is a very positive step in the right direction of looking more comprehensively across these nation-state threats in particular that are targeting all critical infrastructure to make sure that we are empowering industry to learn from how these threats are looking [inaudible].

Mr. OLSON. To echo I agree that from my understanding, I mean, the folks at the Rail Security Alliance represents our private industry and we know they have been talking, TSA has their private briefings we heard that from, Ms. Proctor, earlier that they have been doing Classified briefings for members both in the Passenger Rail Sector and also the Freight Rail Sector. I think there can always be more and more involvement, we have certainly reached out to them to have conversations as well on this point.

What I would say on the what could be done, what could they be doing more is DHS actually has a study sitting at Homeland Security right now that they need to complete by the end of the fiscal year, we would love to work with you all and work with the Department of Homeland Security on this study and ensure that private sectors' voice is heard as they are completing this risk assessment of what state-owned enterprises, how they could affect the U.S. transit and freight rail market.

Mr. RICHMOND. Thank you for your time.

Mr. Chairman, I do have prior commitments so I will yield the balance of my time through the gentleman from Missouri, Mr. Cleaver.

Mr. CORREA. Thank you, Chairman Richmond.

Mr. Cleaver, go ahead.

Mr. CLEAVER. Thank you, Mr. Chairman.

I was mayor of Kansas City all during the 1990's up until 2000 and I can remember one of the most frightening periods of my term as mayor came when we received word, we were not notified but we received word, there was very likely going to be a shipment of [inaudible] and taken to the Nevada, Yucca Mountain and there was a lot of resentment [inaudible] the largest freight-rail site in the country and St. Louis 200 miles away is No. 3.

We are a [inaudible] have been extremely concerned over the years about the transportation of waste but also how vulnerable we are and particularly in the Midwest because you know, no matter what the discussion is, it's probably even freight, we tend to focus on East Coast, West Coast, maybe a little part of the North Coast and the Midwest is wide open.

I always like to remind people that the first major terrorist attack in this country occurred right in the middle—Midwest at Oklahoma City at the Murrah Federal Building. It has nothing to do with rail but the point I am raising, Mr. Lewis, and, Mr. Olson, is that I am not sure that there is any appropriate attention being given to that part of the country where a lot of the rail is centered.

Mr. OLSON. I tend to agree with you, Congressman. I know that you know, the Class Is, the freight rail manufacturers are all working on these issues and working on the cyber aspects of this and the security aspects of this. RSA's position and has been as our concern is allowing the Chinese to come in and make freight railcars——

Mr. CLEAVER. Yes, sir.

Mr. OLSON [continuing]. And be a part of the system and the security challenges come with that. As you know, freight rail carries grain, from toxic waste, to military equipment, and our view is from RSA, as soon as you allow the Chinese into the system and they are building cars they are able to track where all these things are going and get a birds-eye view on where we are moving commodities, we are moving helicopters, where we are moving people and that is of grave concern for us from a National security perspective and we share your concerns sir.

Mr. CLEAVER. Mr. Lewis.

Mr. LEWIS. Thank you, Congressman. You know, I think there's two questions you always want to ask, does the device connect back home and there is a surprising answer to that increasingly as we connect things to the internet. I was reading yesterday about a smart doorbell that was inadvertently relaying peoples' voices back to China so rail cars are a good target, rail lines are a good target, they're traditional military targets, good target for disruption.

The other thing you would want to ask though is when is it in the opponents' interest to do so and in that sense, they are looking at it from a National perspective. They are looking at from where

the least-defended parts of the country, where can they achieve the most effect so in that way may be the Midwest is a good target.

Mr. CLEAVER. Yes. I would argue that there is some evidence to suggest that it is a target and of course my question, Mr. Chairman, is you know, when are we going to give the necessary attention? I mean, you know, when I am asked you know, the question, I am no longer in the mayor's office but the people wants to know, Homeland Security, so when are they going to give us the attention that they have been giving New York and Boston and San Francisco and Los Angeles and I guess I should say, it is still up in the air, until something happens. Is that [inaudible].

Mr. LEWIS. Attention has gone to the largest metropolitan areas and so you are really the top 12 SMSA, Standard Metropolitan Statistical Areas and so the question is, can we expand that? It is a question of cost and also of personnel as we have heard so that tends to mean that if you are not in the top 12, the top 20, you might not be getting the same attention as others.

Mr. CORREA. Thank you, Mr. Cleaver. Thank you very much and I would like to recognize the gentle person from New York, Miss Rice.

Miss RICE. So, Mr. Lewis, just to continue on that so you had said at the beginning right at the end of your original statement, you talked about the cost factor. Can you just expound on that a little bit more?

Mr. LEWIS. Certainly. Thank you. We have heard from the other witnesses too that in many cases Chinese companies are subsidizing—it is part of a larger very aggressive mercantilist policy that the Chinese follow and so that allows them to offer products at a lower price and the information we saw in Australia and them squashing the competition there, you can find that in other industries so you have a subsidized price with pretty good equipment——

Miss RICE. Right.

Mr. LEWIS. Some unknown risk for surveillance or disruption and the buyers have to make a decision, do I pay more for security or do I go with the lower cost and———

Miss RICE. So why is the Federal Government allowing them to make that decision at their level, regardless of whether the money that they are using is State money or Federal money. I mean, I would assume if it is Federal money then we have absolute say over their decision-making process but is it that difference—about what pocket of money they are taking it from?

Mr. LEWIS. We—thank you. We have not come to terms until recently with the fact that there's a risk in buying from China so our supply chains are deeply integrated and so you know, when you go to the store and you turn—very often it will say, Made in China. Up until a few years ago people thought, oh well, you know, they are going to become a market—this is fine, so we have—we are just starting to think about how we disentangle that. Part of it might be asking about what technologies are sensitive, where's there additional risk?

You have all seen all the news on Huawei in the papers and this is a [inaudible].

Miss RICE. What are we waiting for in this field?

Mr. OLSON. I would just add, I mean, Congress did examine this issue last year when it came to Federal Transit Authority dollars, there was actually a 1-year ban put in place in the Senate THUD bill. It was unfortunately stripped out of the final version that you know, you guys passed on February 15 because it was deemed controversial because there are certain members that have state-owned enterprise Chinese facilities in their district and so they are trying to preserve jobs back home.

I will also note—yes, you are right when it comes to the bucket of dollars there are some of these local governments because of the deep discounts that the Chinese are giving, the case of Boston is a very poignant one where the Chinese came in as low as much as 50 percent below some other competitors and so Massachusetts waved FTA dollars, there's no Buy America protections, there's no Federal dollars involved in this project and they have just used State money and therefore the Chinese are able to build many components and the shells and ship them over here so unless we have an outright Federal ban or some Federal law that says, you can't do this, I would assume that States continue to buy because of price.

Miss RICE. So I am just wondering how we sound the alarm bell. I mean, I just don't know, if we are allowing elected Members of Congress to be more concerned about preserving jobs in their districts than they are a National security, we have a problem so if you wouldn't mind, Mr. Olson, just talking a little bit, can you just expound on that more because this has to be done. If this administration does not think that this is a priority, it is not going to trickle down, it is just not.

Mr. OLSON. I agree with you wholeheartedly. We are a 3-year-old organization. We started because we saw this market entry in such a quick fashion and the 4 contracts quickly awarded to CRRC. They have built a freight assembly facility in Wilmington, North [inaudible] so opportunities like this to testify and get in front of more Members, I mean, we are advocacy; we are trying to get in front of as many Members of Congress, and State and local officials to raise the alarm bells and we are partnering as much as possible with officials within the Trump administration to raise more awareness.

Miss RICE. Well, I want to thank Chairman Correa, very much for actually you know, putting this hearing together.

I want to thank all of you so much because we sit here in this little bubble here in Washington and you know, the very common theme that I have heard from everyone who has sat at that table is, we have to keep the lines of communication open. This is not a private-sector issue. This is not a public-sector issue. This is a Keep America Safe issue, and Our Democracy Safe issue, and I hope that you know, going forward and I know with people like you will be able to; I hope we can have this conversation in a bipartisan fashion so thank you all for being here.

I yield back the balance of my time.

Mr. CORREA. Thank you, Miss Rice. I agree with you about sounding the alarm. It is a very interesting question.

Now I would like to recognize, Mrs. Watson Coleman, from New Jersey.

Mrs. WATSON COLEMAN. Thank you. Thank you, Mr. Chairman.

So if we have these companies that are owned by the Chinese company making things in the United States of America, technically we could have professionals from security, cybersecurity whatever to be able to go in, announced and unannounced and check right——

Mr. OLSON. Of course.

Mrs. WATSON COLEMAN. We probably could?

Mr. OLSON. Yes.

Mrs. WATSON COLEMAN. Do we? Do you know, if we do?

Mr. LEWIS. It does not work and so that is the main problem.

Mrs. WATSON COLEMAN. It does not work, why?

Mr. LEWIS. It does not work because first a lot of the—it never did.

Mrs. WATSON COLEMAN. Yes.

Mr. LEWIS. Pardon me. A lot of the technology is connected back to the manufacturer——

Mrs. WATSON COLEMAN. OK.

Mr. LEWIS. So that they can do updates; you don't know if it is malicious traffic or innocent traffic. Second there is just a lot of opportunities in rail car or an airplane to hide——

Mrs. WATSON COLEMAN. We are just trying to figure this out.

You know, Mr. Olson, this one paragraph [inaudible] what do you think the Federal Government's role should be here in ensuring that this does not happen here?

Mr. OLSON. So first off, RSA's continued position is, taxpayers' dollars should not be used to be subsidizing the state-owned enterprise from China period, end of story.

Second, I would love to work with all of you as we look at other ways to do bans or outright bans on this technology from being on our system. I think it is too scary to allow Chinese government-directed company to operate in the United States especially when they are building a good chunk of the materials in China itself.

Mrs. WATSON COLEMAN. Because the interest actually is not blowing us up as it is much as just owning us?

Mr. OLSON. Tracking us.

Mrs. WATSON COLEMAN. Owning us.

WMATA which oversees the Washington Metro System was currently working to procure new rail cars and updates its procurement requirements to include the enhanced [inaudible] safeguards.

Mr. OLSON. RSA's position is as, Mr. Lewis, stated, it is never enough. If you are going to be building components and parts in China, you can never do enough to mitigate. Our position at RSA continues to be risk avoidance, let's just not buy them.

Mrs. WATSON COLEMAN. So let's not allow our money to be spent on purchasing Chinese——

Mr. OLSON. Correct.

Mrs. WATSON COLEMAN. OK.

I am good. Thank you.

I yield back.

Mr. CORREA. Thank you very much for those questions.

Now I would like to recognize the good lady from Texas, Ms. Jackson Lee.

Ms. JACKSON LEE. Thank you very much Mr. Chairman.

Having just come in, let me first of all thank the witnesses of the first panel and thank those of the second panel [inaudible] events I have been on this committee since 9/11 and have seen the maturing of terrorist potential and utilization of now technology different from bringing down a plane or using it as a torpedo into major structures here in the United States, though it certainly is well-known that certain elements still believe that aviation is a crucial and serious part, but I would be interested—or infrastructure is a crucial and serious part of potential of attacking the United States.

So, I am going to ask each of your question as to whether or not you are—do you think we are fully prepared for zero-day potential events; start with, Ms. Gagliostro?

Ms. GAGLIOSTRO. So I would say, in dealing with any sort of cybersecurity threats, the most important way for us to be prepared and respond is through working with our Federal partners on having strong information sharing on what we are learning so zero-day threats are always a challenge because it is what you don't know yet but I think being cognizant of the threat indicators and patterns of behavior and paying attention to those that we can be alerted to those threats quickly as possible.

Ms. JACKSON LEE. You think the United States should address those questions through legislation that would emphasize the partnership between the Federal Government and the private sector?

Ms. GAGLIOSTRO. I think the best way to address that is through strong partnership between the Federal Government and the private sector.

Ms. JACKSON LEE. So legislation that dictates that would be helpful?

Ms. GAGLIOSTRO. To the extent that we don't think it is effective today.

Ms. JACKSON LEE. Mr. Lewis.

Mr. LEWIS. Thank you. First, I would distinguish between state and non-state actors. No terrorist group currently has the capability nor will acquire in the foreseeable future the capability to launch a damaging cyber attack. This has been true for years, it is based on evidence from a number of——

Mr. CORREA. Could you repeat that please?

Mr. LEWIS. No terrorist group currently has the capability to launch a damaging cyber attack.

Ms. JACKSON LEE. But please know that my zero-day is not limited to nation-states.

Mr. LEWIS. Exactly right. We have 4 very capable opponents who have certainly done the reconnaissance to launch these kinds of attacks against——

Ms. JACKSON LEE. Why don't you just recite their names for the records?

Mr. LEWIS. Russia, China, Iran, and North Korea, right, they all have the capability, it is a question of when they would use it so on the defensive side all the work that you have heard from my colleagues, perhaps some improvement in standards.

On the offensive side, as we discussed earlier [inaudible].

Ms. JACKSON LEE [continuing]. Be effective focusing the Government on those issues?

Mr. LEWIS. Ma'am, I have asked senior officials at DHS, if they need more legislative authority, their position is no, but I think it would be useful to look and see where there are gaps in the existing legislation that might help them do better at protecting———

Ms. JACKSON LEE. Then they do need it because there are gaps.

Mr. OLSON [continuing]. And then, Mr. Hultquist, you follow?

Mr. OLSON. I would agree with my colleagues on the panel here and we would not oppose further legislation if it gives more authority to fill as you said gaps for DHS.

You know, our position from the Rail Security Alliance is that we have already allowed the Chinese in and that we need to stop the bleeding and not have them further infiltrate more transit systems and especially the freight systems so we are looking at it from that angle of hardware in the United States already.

Ms. JACKSON LEE. Thank you.

Mr. HULTQUIST. We have had good success anticipating a lot of these events by looking at the places where these actors are most active—Ukraine, the Middle East, South Korea—so I would argue that getting that information, the observables out of those spaces to the private sector who would likely bear the brunt of any attack is probably the most important thing we can do.

Ms. JACKSON LEE. So if you have any legislation that focuses on some of the elements that you have just mentioned——

Mr. HULTQUIST. Absolutely, enforcing public-private partnership I think would be really important.

Ms. JACKSON LEE. Just last question, Mr. Chairman, cybersecurity is becoming harder because of the connected nature of wireless technology, how long can we secure large complex systems when very small devices can pose risks? Whoever feels most capable to answer that question, I would be delighted.

Mr. LEWIS. I will start. We can't secure them now so it is hard to see how it gets much worse but I think that as you add more and more connected devices, the ability to create some sort of havoc—we talked about the smart doorbells.

Another one I just heard about is you know, those visible braces you have got? Some of them are connected to the internet and you can just think of endless numbers of complications, between smart cars, smart ships, robots; they are moving into a world where the number of things that can be hacked is growing exponentially.

Ms. JACKSON LEE. Thank you.

So anyone else on how do we—yes sir?

Mr. HULTQUIST. We add more potential for disruption but we also add more factors for the threat actors to gain access to critical systems or systems that we care about.

Ms. JACKSON LEE. Anyone else.

Mr. Chairman, I will just conclude by saying that there are gaping holes with our cyber system. This committee is best suited to try to address those questions and gaping holes can create opportunities for havoc and I think this committee and the Oversight on Transportation, Natural Gas, is crucial in its work and I hope we will pass legislation dealing with some of these very large holes that——

Mr. CORREA. I concur with you, Ms. Jackson Lee, and I think——

Ms. JACKSON LEE. They create danger.

Mr. CORREA. We have got a job to do here in terms of addressing those gaping holes.

It seems like every time we turn around there is a new toothbrush with a chip on it so when you are brushing your teeth somebody's going to know how many times you do it a day and my point is there is no privacy anymore and it looks like all of our information is interconnected in some form or another, whether it is a commercial venture, a state somewhere around the world so, Mr. Lewis, you intrigue me again with your comments about the deterrence, is there a price to pay for what and when, and when does that trigger?

Good questions.

I want to thank all the witnesses for their valuable testimony and all the Members here for their questions.

The Members of the committee may have additional questions for the witnesses and we ask that you respond to them expeditiously and in writing. Pursuant to Committee Rule VII(D), the hearing record will be held open for [inaudible].

Thank you to all the committee Members, of both committees, or I should say panels.

We stand adjourned.

[Whereupon, at 12:22 p.m., the subcommittees were adjourned.]

○